Artikkeli

VERTAISARVIOITU
KOLLEGIALT GRANSKAD
PEER-REVIEWED
www.tsv.fi/tunnus

Kyberturvallisuus valtiollisena toimintaympäristönä ja siihen kohdistuvat uhkat

Toimivat tietoliikenne- ja viestintäjärjestelmät ovat digitaalisessa maailmassa tärkeä osa yhteiskunnan perusinfrastruktuuria, mutta ne eivät ole riippumattomia poliittisista ideologioista, kansallisvaltioiden päämääristä tai kaupallisista intresseistä. Tässä teoreettisessa artikkelissa tätä infrastruktuuria tarkastellaan käsitteellistäen se kybertoimintaympäristöksi. Koska kybertoimintaympäristön olemassaolo määrittyy erilaisten uhkien kautta, kohdistuu kiinnostuksemme ennen muuta kyberturvallisuuteen. Tämän artikkelin tavoite on yhtäältä analysoida kyberturvallisuuden käsitettä ja toisaalta luoda ymmärrystä siitä, miten valtiolliset strategiatekstit ja uutistekstit osaltaan rakentavat kyberturvallisuutta toimintaympäristönä. Tutkimuksessa osoitetaan, että kyberturvallisuus on tietoverkkojen ydintoimintoihin kytkeytyvä mutta ristiriitainen ilmiö. Kyberhyökkäyksiin liittyvä uutisointi keskittyy sekä uhkien hallitsemattomuuteen että vahvoihin toimijoihin, jotka taistelevat niitä vastaan. Kyberturvallisuusstrategiat taas ovat keino hälventää ristiriitaista käsitystä valtioista kansalaisten valvojina ja vakuuttaa heidät siitä, että valtion toimet kybermaailmassa ovat heidän parhaakseen.

AVAINSANAT: Kybertoimintaympäristö, kyberturvallisuus, kyberstrategia, uhka, tietoverkot, internet, informaatiovaikuttaminen

Keväästä 2017 lähtien Suomessa on keskusteltu kiivaasti tiedustelulainsäädännön uudistuksesta (esim. Halminen & Pietiläinen 2017a, 2017b; Happonen 2017; Leipola 2017; Tolkki 2017). Suomen sisäministeriö ja puolustusministeriö julkistivat 19.4.2017 luonnokset laeiksi, jotka mahdollistaisivat entistä laajemmat valtuudet sekä puolustusvoimille että suojelupoliisille erityisesti maan rajat ylittävän internetliikenteen seurantaan (Sisäministeriö 2017b). Siviilitiedustelulainsäädännön muutosta valmisteltiin yhteistyössä ja samaan aikaan kun puolustusministeriössä tehtiin soti-

lastiedustelua ja oikeusministeriössä perustuslain mahdollista muuttamista koskevia lainsäädäntöhankkeita (Sisäministeriö 2017a). Jo helmikuussa 2017 valtioneuvoston julkistamassa puolustusselonteossa oli korostettu, miten digitalisoitunut toimintaympäristö asettaa uusia vaatimuksia tiedustelutietojen hankinnalle ja kyberpuolustukselle (Puolustusministeriö 2017b). Käytännössä selonteossa viitataan kyber- ja informaatiovaikuttamiseen, joita vastaan taistelemisessa tiedustelu- ja vakoilutoiminnalla on merkittävä rooli (ks. Leipola 2017).

Tietoliikennettä, viestintää ja tiedustelua koskevilla poliittisilla kysymyksillä on keskeinen rooli tulevaisuuden digitaalista yhteiskuntaa rakennettaessa. Yksi ratkaiseva kipukohta niissä näyttää liittyvän perustuslain turvaamaan yksityisyyden suojaan, viestinnän salaisuuteen ja sananvapauteen, joita tietyin edellytyksin voidaan kaventaa muun muassa poliisilain (872/2011) ja pakkokeinolakiin 1.1.2014 voimaan tulleiden muutosten (1467/2011) perusteella (ks. Viljanen 2017). Pakkokeinolaki antaa nykyisellään poliisille muun muassa oikeuden tarkkailla epäillyn internetviestintää tämän koneelle asennetun haittaohjelman avulla. Käynnissä olevassa ja kiireelliseksi julistetussa (ks. Rydman 2017) tiedustelulainsäädännön uudistusprosessissa yksilön oikeuksista viestintään – informaation lähettämiseen ja vastaanottamiseen kenenkään estämättä – joudutaan tavalla tai toisella tinkimään. Tämä prosessi ei ole lehtitietojenkaan mukaan aina sujunut kitkatta; esimerkiksi vuonna 2015 uutisoitiin, että liikenne- ja viestintäministeriö vastusti kiivaasti tuolloin käsittelyssä ollutta verkkovalvonnan mahdollistanutta lakiehdotusta (Kauhanen 2015). Kyse onkin lopulta poliittisista päätöksistä, joiden puntaroinnissa joudutaan toisinaan asettamaan vastakkain yksilön ja yhteiskunnan etu.

Toimivat tietoliikenne- ja viestintäjärjestelmät ovat digitaalisessa maailmassa tärkeä osa yhteiskunnan perusinfrastruktuuria. Ne eivät kuitenkaan ole autonomisia suhteessa poliittisiin ideologioihin, kansallisvaltioiden päämääriin tai kaupallisiin intresseihin. Näistä erilaisista mutta yhteenkietoutuvista toimintalogiikoista esimerkkinä voi tarkastella vaikkapa pankkien ylläpitämää sähköisen tunnistautumisen järjestelmää, joka toimii edellytyksenä verkkotoimijuudelle (mm. verohallinnon ja sosiaaliturvan palvelut) ja poliittiselle osallistumiselle (mm. vetoomusten allekirjoittaminen internetissä). Myös internetin käytön kulttuurit ja käyttäjien keskenään ristiriitaiset pyrkimykset vaikuttavat tämän infrastruktuurin rakentumiseen. Infrastruktuuria koskevasta lainsäädännöstä ja sen poliittisista perusteista on tärkeä käydä julkista keskustelua myös muilla kuin varsinaisesti juridiikkaa käsittelevillä foorumeilla.

Tässä artikkelissa tätä infrastruktuuria tarkastellaan käsitteellistäen se *kybertoimintaympäristöksi*. Kybertoimintaympäristö koostuu useista toisiinsa yhdistyneistä tietoverkoista, joissa tietoa siirretään digitaalisessa muodossa käyttäjältä ja koneelta toiselle, tietoliikennetekniikasta, tietokoneista sekä eri tehtäviä hoitavista datasäilöistä, reitittimistä ja palvelimista. Näin se määritellään esimerkiksi Yhdysvaltain presidentin George W. Bushin aloitteesta syntyneessä linjauksessa kansallisen kyberturvallisuuden takaamiseksi (*Comprehensive National Cybersecurity Initiative*, CNCI) (ks. The White House 2008). Kybertoimintaympäristöön kuuluu lisäksi olennaisena osana ihminen, joka ainakin vielä toistaiseksi vastaa verkon ylläpidosta ja sen toimintaedellytyksistä (ks. Sessions 2014).

Koska kybertoimintaympäristön olemassaolo yhteiskunnallisessa kontekstissa määrittyy erilaisten uhkien kautta, kohdistuu kiinnostuksemme tässä artikkelissa ennen muuta *kyberturvallisuuteen*, joka määritellään Suomen kyberturvallisuusstrategiassa (Puolustusministeriö 2013, 13) "tavoitetilaksi, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan". Kun kybertoimintaympäristön ajatellaan aikaisemman määritelmän mukaisesti koostuvan teknologiasta, informaatiosta ja ihmistoimijoista, kyberturvallisuus takaa näiden kolmen tason turvallisuuden ja varmistaa, ettei kybertoimintaympäristössä olevan informaation käsittelystä koidu vaaraa tai häiriötä sen toiminnalle. Omat haasteensa kyberturvallisuudelle asettaa uhka *informaatiovaikuttamisesta* tai *informaatiosodankäynnistä*, joka ei varsinaisesti häiritse kybertoimintaympäristön teknologista toimintavarmuutta, mutta jossa informaatiota käytetään strategisena keinona vaikuttaa valtion tai kansalaisten päätöksentekoon ja siten ihmisten toimintaan (Valtioneuvoston kanslia 2004, 156). Informaatiosodankäynnin keskeiset alueet voidaan yleisesti jaotella tiedusteluun, vaikuttamiseen ja johtamiseen (Jantunen 2015, 20).

Kyberturvallisuus on siis tapa tarkastella yhteiskunnallisella tasolla tietoliikenne- ja viestintäjärjestelmien toimivuutta ja toiminnan turvaamista. Kyberturvallisuuteen liittyy teknologisten näkökohtien lisäksi myös laajoja poliittisia kysymyksiä, jotka tekevät tästä aihepiiristä kiehtovan erityisesti yhteiskuntatieteellisesti orientoituneessa viestinnän tutkimuksessa. Vain ne huomioimalla on mahdollista lisätä ymmärrystä esimerkiksi valeuutisten (*fake news*), trollien ja vihapuheen kaltaisista pinnalla olevista kulttuurisista ilmiöistä, jotka omalta osaltaan vaikuttavat julkisen keskustelun luonteeseen. Silloin kun tutkimusasetelma laajennetaan valtiollisen tai kansainvälisen tason kysymyksiin, kuten poliittisesti motivoituihin haittaohjelmiin, tietovuotoihin tai tiedustelutiedon (väärin)käyttöön, tietoliikenne- ja viestintäjärjestelmien sekä niiden julkisoikeudellisen sääntelyn tuntemus lienee väistämättä osa analyysin rakentumista.

Tämän teoreettisesti suuntautuneen artikkelin tavoite on yhtäältä analysoida kyberturvallisuuden käsitettä edellä hahmotellussa laajassa kontekstissa ja toisaalta luoda ymmärrystä siitä, miten strategia- ja uutistekstit osaltaan rakentavat kyberturvallisuutta toimintaympäristönä. Nostamme esiin valtiollisella tasolla tuotettuja strategiatekstejä, joissa kybertoimintaympäristöä ja siihen liittyviä uhkakuvia pyritään ottamaan haltuun kansallisella tasolla, sekä kyberrikollisuuteen ja informaatiovaikuttamiseen keskittyviä viimeaikaisia uutisia. Emme analysoi tekstejä empiirisesti vaan käytämme niitä esimerkinomaisesti todentamaan teoreettista hahmotelmaamme kyberturvallisuuden rakentumisesta yhteiskunnallisena ilmiönä.

Valtioiden tuottamat kyberturvallisuusstrategiat ovat syntyneet vastauksena digitaalisten järjestelmien mukanaan tuomiin ongelmiin ja koettuihin uhkiin (ks. Jansson 2017). Strategiatekstit on koottu syksyllä 2016 Naton kyberpuolustusyksikön verkkosivuilta, jonne on listattu eri maiden kyberturvallisuusstrategiat (CCDCOE 2016). Tarkastelemamme media-aineisto puolestaan kattaa 23 uutisjuttua, joissa on käsitelty kyberturvallisuuteen liittyviä kysymyksiä ja jotka on kerätty kotimaisten tiedotusvälineiden verkkosivuilta vuosilta 2016–2017. Juttuja ovat julkaisseet muun muassa *Helsingin Sanomat*, Yle, *Uusi Suomi* ja *Verkkouutiset*. Koska kyberturvallisuus tutkimuksen

kohteena on maailmanlaajuinen ilmiö, suomalaista uutisointia on täydennetty 17 kansainvälisellä viitteellä, joihin lukeutuu esimerkiksi BBC:n, Reutersin, *Washington Postin* ja *The Guardianin* verkkoversioissa julkaistuja juttuja.

Yhteiskunnallisesta merkittävyydestään huolimatta kyberturvallisuuden tutkimus on toistaiseksi ollut vähäistä. Kyberturvallisuusstrategioita ovat aiemmin tutkineet Luiijf, Besseling, Spoelstra ja de Graaf (2011) sekä Luiijf, Besseling ja de Graaf (2013) vertaamalla erilaisista aineistoista käsin valtioiden heikkouksia ja mahdollisuuksia kybermaailmassa. Myös ei-valtiolliset organisaatiot, kuten ENISA (2014) ja OECD (2012), ovat julkaisseet raportit strategioiden pääpiirteistä. Suomessa Jarno Limnéll kumppaneineen on tehnyt kyberturvallisuudesta ja -sodasta useita tutkimuksia vuosina 2014–2016. Kyberstrategioita on aiemmin tutkinut myös Aleksi Saloharju (2015) pro gradussaan, jonka näkökulma on kyberturvallisuuskäsityksissä ja alueellisissa eroissa, sekä tämän artikkelin toinen kirjoittaja Saara Jansson (2017), jonka pro gradu -työn avaamaan kontekstiin myös tämä artikkeli tukeutuu. Kuten on havaittavissa, kybertoimintaympäristöjen tutkimus on kansainvälisestikin vasta kehkeytymässä, eikä kyberturvallisuuteen liittyvälle yhteiskuntatieteelliselle keskustelulle ole Suomessa toistaiseksi ollut luontevaa paikkaa.

Näitä keskusteluja on kuitenkin tärkeä käydä, sillä kybermaailma ei ole vain teknologisen kehityksen huipentuma, vaan ”strateginen ja poliittinen asia, jossa ’ison kuvan ja suunnan määrittämisen’ ymmärrys on valitettavan heikkoa” (Limnéll ym. 2014, 14). Toisin sanoen kyberturvallisuuteen liittyvissä keskusteluissa on kyse muustakin kuin teknologiasta: niiden tulisi keskittyä historiatajuisen ja poliittisesti orientoituneen ymmärryksen luomiseen maailman tilasta, valtioiden välisistä suhteista ja eri valtioiden roolista kansainvälisen yhteisön rakentumisessa (ks. Naughton 2016a). Tässä artikkelissa pyrimme keräämään aineksia juuri tällaisen “ison kuvan” määrittämiseen tarkastelemalla käytettyjä käsitteitä, uhkakuvien luomista ja uhkien moniulotteisuutta kyberturvallisuusdiskurssissa. Kyberturvallisuutta käsittelevien tekstien analyysissa on olennaista, miten poliittisella tasolla perustellaan siihen panostamista ja toisaalta millaisia uhkia valtioiden tulevaisuudessa uumoillaan olevan (ks. Rudner 2013). Työtämme läpileikkaava kysymys on myös se, millaisia rooleja eri toimijoille hahmottelemassamme kyberturvallisuutta käsittelevässä keskustelussa asemoituu. Näitä teemoja ajatellen tarkastelemme artikkelin loppupuolella kahta yksittäistä ilmiötä: kyberrikollisuuden käsittelyä uutisteksteissä sekä informaatiovaikuttamisen ja median välisiä kytköksiä.

Kyber-käsitteiden ja tietoverkkoinfrastruktuurin historiaa

Jarno Limnéllin, Klaus Majewskin ja Mirva Salmisen (2014, 16–17, 20–21) mukaan kyberturvallisuudesta on tullut pysyvästi yksi valtioiden turvallisuuspolitiikan alueista. Muutos on tapahtunut nopeasti, sillä pelkästään internetin valtavirtaistumisesta on vasta alle kaksikymmentä vuotta. Jatkuvasti muuttuva kybermaailma ja sen turvaaminen vaikuttavat valtioiden välisiin suhteisiin ja siihen, mitä eri kybermaailman toimijat

osaltaan tavoittelevat. Vaikka kybertoimintaympäristö ja siihen liittyvät ilmiöt ovat käytännön tasolla uusia, kyber-alkuisiin käsitteisiin kytkeytyvät puhetavat itsessään ovat paljon vanhempia. Eräänlaista diskursiivista arkeologiaa harjoittamalla Michael Warner (2012) päätteleekin, että puolustuspolitiikkaa ohjaava "kyberdiskurssi" on ilmennyt lukuisissa eri julkisissa puheenvuoroissa ja keskusteluissa jo vuosikymmeniä ennen sen varsinaista läpimurtoa populaarijulkisuuteen 1990-luvulla.

Voidaksemme tässä artikkelissa tarkastella tietoliikenne- ja viestintäjärjestelmien rakentumista kansalliseksi kybertoimintaympäristöksi luomme seuraavaksi katsauksen kyber-alkuisten termien käsitteelliseen historiaan. Kyber-etuliitteen historia yltää 1940-luvulle saakka ja sitä seuranneiden vuosikymmenien aikana sen merkitys on muuttunut useaan otteeseen. Ensimmäisenä käsitettä käytti Norbert Wiener teoksessaan *Cybernetics: Or Control and Communication in the Animal and the Machine* (1948), jossa hän yhdisti viestintää teknologian ohjaukseen ja havaitsi, että ihmisellä on merkittävä rooli koneiden hallinnassa. Hän nimesi uuden tieteenhaaransa *kybernetiikaksi*, joka tulee kreikan kielen sanasta *kybernētēs* (perämies). (Mindell 2003, 4.) Sen kantasanana toimii muun muassa *kybereo*, joka tarkoittaa ohjaamista, opastusta tai hallintaa (Limnéll ym. 2014, 29). Alkujaan kyber-etuliitteellä viitattiin siis ihmisen ja koneiden väliseen vuorovaikutukseen ja viestintään, jossa ihminen toimi ohjaajana.

Vaikka kyberin tausta juontuu kybernetiikasta, ei se enää tarkoita ihmisen tulemista osaksi koneita ja niiden kontrollointia. Käsitteen uudelleenmäärittely on kesken, ja toisinaan alan tutkijat jopa kieltäytyvät määrittelemästä sitä (ks. esim. Limnéll 2014, 3–4; Hamilton 1998, 179). Singer ja Friedman (2014, 13) määrittelevät kybertoimintaympäristön koostuvan "verkossa olevien tietokoneiden valtakunnasta, jossa tietoa varastoidaan, jaetaan ja kommunikoidaan online-tilassa" – mukaan lukien verkon ja koneiden käyttäjät. Myös Limnéllin ym. (2014, 30–31) mielestä ihmisen toiminta kuuluu olennaisesti kybertoimintaympäristöön. Heidän mukaansa käsitteelle on ollut tarve määritettäessä uudenlaista toimintaympäristöä, jossa ihmisellä on erilaisia toiminnan mahdollisuuksia ja toisaalta uhkia, joita fyysisessä maailmassa ei ole.

Erona Limnélliin ym. (2014) Singer ja Friedman pohtivat laajemmin kybertoimintaympäristön fyysisiä ulottuvuuksia. Heidän mukaansa kybertoimintaympäristö ei ole maantieteellisesti tai millään muullakaan määritelmällä rajaton. Valtiot hallinnoivat toimintaympäristöä maiden rajojen sisäpuolella, ei-valtiolliset organisaatiot taas jotakin muuta globaalin verkon osa-aluetta. Lisäksi kybertoimintaympäristöä määrittää jatkuva muutos ja laajeneminen. Jos alussa se näyttäytyikin pelkästään tiedonsiirron välineenä, 2010-luvulla kaikki valtioiden kriittisimmät infrastruktuurit toimivat kybermaailmassa aina sähkö- ja vesilaitoksia sekä liikenteenohjausta myöten. (Singer & Friedman 2014, 14–15.) Vaikka digitaalinen teknologia ja tietoverkot ovat nykyään erottamaton osa arkeamme ja myös kansallisvaltioiden olemassaoloa, niiden historia on laajemmassa katsannossa yllättävän lyhyt. Internet levisi laajan yleisön käyttöön 1990-luvun lopulla, mutta varsinaisen liiketoiminnan voidaan katsoa alkaneen vasta seuraavalla vuosikymmenellä (Naughton 2016b, 18). Sosiaalinen media ja älypuhelimet, jotka ovat erottamaton osa kansalaisten arkea 2010-luvun lopulla, esiteltiin vain hieman yli kymmenen vuotta sitten. Kuuluisimmat kyberhyökkäykset ja haittaohjel-

matkin sijoittuvat viimeisen vuosikymmenen sisään (esim. Moore 2017). Kyberilmiöiden uutuudesta kertoo jotain se, että vasta 2010-luvulla on voitu spekuloida, mihin suuntaan kybermaailma mahdollisesti on kehittymässä (Limnéll 2014, 16–17).

Vaikka kyber-alkuiset käsitteet ovat muuttuvia ja monitulkintaisia, muun muassa Suomen puolustusvoimien kyberjaoston päällikkö Catharina Candolin (2012) puolustaa niiden käyttöä. Hänen mukaansa ”kyberistä” keskusteltaessa yleinen mielipide on, että sitä ei pitäisi käyttää, mutta toisaalta kukaan ei ole tarjonnut tilalle parempaakaan käsitettä. Kyberille tarjotut vastineet, kuten tietoverkko, tietoturvallisuus tai tietoverkkoturvallisuus, eivät kata kokonaisuudessaan kaikkea sitä, mihin kyberillä viitataan. Koska tämän tutkimuksen tavoitteena ei ole tehdä varsinaista käsiteanalyysia kyberistä eikä keksiä uutta termiä sen tilalle, käytämme kyber-alkuisia sanoja ja ilmaisuja viitataksemme ihmisen aikaansaamaan toimintaympäristöön, johon linkittyvät ihmisyhteisöt, koneet, infrastruktuurit ja kaikki toiminnan mahdollistavat instituutiot. Määrittelemme kybermaailman tai kybertoimintaympäristön digitaaliseksi tilaksi, jolla on myös materiaalisia ulottuvuuksia, joissa dataa konkreettisesti varastoidaan ja siirretään, ja jota on diskursiivisesti pohjustettu erityisesti sotilaallisissa ja puolustuspoliittisissa yhteyksissä jo vuosikymmenten ajan (ks. Warner 2012). Kybertoimintaympäristö on kansallisen tason konteksti, jonka suojaamiseen käytetään kyberturvallisuutta.

2010-luvulle tultaessa kyberturvallisuudesta on tullut myös näkyvä politiikan teon väline, joka ilmenee tämänhetkisessä julkisessa keskustelussa monin eri tavoin. Valtiot ovat kiinnostuneita kybermaailman strategisista mahdollisuuksista, mutta toisaalta kyberturvallisuudesta on monissa maissa tullut puolustuspolitiikan kulmakivi ja yksi sodankäynnin ulottuvuuksista. Esimerkiksi Yhdysvallat ilmoitti vuonna 2013 suurimmaksi kansallista turvallisuuttaan uhkaavaksi tekijäksi kyberuhkat terrorismin sijasta (Limnéll ym. 2014, 20). Kyseessä on iso strateginen muutos, sillä Yhdysvallat on maailman johtava sotilaallinen supervalta. Suomessakin näistä asioista on vuonna 2017 käyty runsaasti keskustelua, jossa Turussa 18.8.2017 tapahtunut puukkohyökkäys ja “tiedustelulaiksi” nimetty kyberuhkia torjuva lainsäädännön muutos kytketään yhteen (esim. Incoronato 2017; Miikkulainen 2017; Mäntymaa 2017).

Turvallisuuspolitiikan ohella myös muita yhteiskunnan perustoimintoja voi ajatella kybermaailman näkökulmasta. Esimerkiksi Viro myöntää e-kansalaisuuksia, joiden avulla kansalaiset saavat ikään kuin digitaalisen identiteetin ja jotka helpottavat yrityksen perustamista (e-Estonia 2017). Suomessa taas on mahdollista tunnistautua verkkopankkitunnuksilla moniin julkisyhteisöllisiin palveluihin, kuten vero-, sosiaali- etu- ja potilastietokantoihin (Suomi.fi 2017). Kun iso osa valtion tarjoamista palveluista on digitalisoitunut ja siirtynyt verkkoon, voidaan sanoa, että valtiot ovat siirtyneet ”kyberaikakauteen” – jolla ei tässä yhteydessä viitata yleisesti digitalisoitumiskehitykseen vaan yhteiskunnan perustoimintojen digitaaliseen uudelleenorganisoitumiseen, julkishallinnon erityiskysymyksiin sekä kansalliseen ja kansainväliseen politiikkaan tämän kehityksen kontekstina. Esimerkiksi demokraattisiin vaaleihin liittyvä arkaluontoinen tieto voi houkutella vakoilijoita, tietoverkkorikollisia ja tiedusteluorganisaatioita etsimään keinoja päästä siihen käsiksi. Tämä on vaatinut valtioita kehittämään

kyberpuolustusta, jonka avulla ne suojelevat kansalaisiaan ja omaa suvereniteettiaan. Valtioilla on merkittävä rooli kyberturvallisuuden ylläpitämisessä, sillä esimerkiksi tieto- ja viestiliikenneverkot kuuluvat valtiollisesti valvottavaan infrastruktuuriin (ks. Shackelford & Craig 2014). Suomessa tehtävää hoitaa Viestintävirasto sekä sen alaisuudessa toimiva Kyberturvallisuuskeskus, joka valvoo tieto- ja viestiliikenneverkkojen toimivuutta ja turvallisuutta. Kriittinen tietoverkkoinfrastruktuuri on erillisen, valtio-omisteisen yhtiön Suomen erillisverkot Oy:n hallinnassa.

Kybertoimintaympäristöön ja kyberturvallisuuteen liittyy olennaisesti internet. Internetiä käytetään usein jopa synonyymina kybertoimintaympäristölle, sillä internet on ikään kuin konkreettinen väline ja keino niille toimenpiteille, joiden kautta kybertoimintaympäristö tulee olemassa olevaksi. Modernissa internetissä on kyse tiedonsiirrosta useiden erillisten verkkojen välillä. Vaikka internetiä ajatellaan usein yhtenä ja yhtenäisenä, koko maailman kattavana kokonaisuutena, todellisuudessa se koostuu useista alaverkoista ja pienemmistä alueellisista verkoista (Naughton 2016b, 6). Nämä alueelliset verkot vaihtavat ja välittävät viestejä yhteisen teknisen kielen avulla, mikä mahdollistaa koko internetin toiminnan (Singer & Friedman 2014, 18). Monilla erillisillä verkoilla on kuitenkin oma toimintalogiikkansa, kuten Tor-verkolla, joka takaa niin sanotun sipulireitityksen avulla käyttäjilleen täyden anonyymiyden ja sensuurin kiertämisen. Tässä tutkimuksessa internet nähdään ensisijaisesti välineenä, jonka avulla data liikkuu kybertoimintaympäristössä ja johon useat kyberturvallisuutta koskevat toimenpiteet kohdistuvat.

Yksittäisten alaverkkojen olemassaolo täytyy kokonaisuuden rakentumisessa kuitenkin ottaa huomioon. Perinteisesti internetin historia ajoitetaan alkamaan ARPANETistä. Vuonna 1969 käyttöönotettu ARPANET oli Yhdysvaltojen puolustusministeriö Pentagonin ja tiedeyliopistojen yhteinen hanke tehokkaamman tiedonsiirron toteuttamiseksi näiden eri instituutioiden välillä (Singer & Friedman 2014, 17). Mediahistorioitsija James Curranin (2012, 36–38) mukaan Pentagon halusi rakentaa teknologian, joka kestäisi Neuvostoliiton mahdollisen hyökkäyksen ja jonka avulla puolustusvoimien kalusto – maa- ja ilmavoimat sekä laivasto – pysyisi kaikissa tilanteissa keskenään kommunikaatioyhteydessä. Tiedeyhteisölle taas oli tärkeää, että pääsy verkkoon ei olisi keskittynyt vain tiettyyn paikkaan. Yhteinen tavoite toi kumppanit yhteistyöhön, kunnes Vietnamin sodan myötä esiin nousseet kysymykset verkon turvallisuudesta pakottivat tietoverkkoinfrastruktuurin jakamiseen puolustusvoimien (MILNET) ja tiedeyhteisön (uusi ARPANET) kesken. Tämän jälkeen molempia verkkoja kehitettiin autonomisesti sotilasverkon jäädessä salaiseksi. Yhdysvaltain puolustusvoimissa toteutettu kehitystyö ja siihen liittyvät protokollat tietoverkkoja varten jäävät internetin historiankirjoituksessa usein vähäiselle huomiolle. Tietoverkkojen puolustuspoliittiset juuret on kuitenkin tärkeä tiedostaa erityisesti tarkasteltaessa kybertoimintaympäristön muotoutumista (ks. Schjolberg 2014, 13–14).

Siinä missä puolustusvoimien tietoverkkohanke salattiin, avautui tiedeyhteisön verkko jatkuvasti yhä laajemmalle yleisölle. Varhaisen internetin käyttäjät olivat samalla sen luojia ja kehittäjiä, ja heitä kiehtoi uudessa teknologiassa ensisijaisesti se, että he pääsivät itse muokkaamaan sitä (Naughton 2016b, 8–9). Tällaisten muokat-

tavien eli generatiivisten teknologioiden ideana on, että käyttäjällä on mahdollisuus toteuttaa itseään niiden avulla, harrastaa niitä sekä innovoida ja leikkiä niillä. Internetin kehittäjistä muodostui yhteisö, joka halusi oma-aloitteisesti parantaa generatiivista verkkoa. Internet kasvoi pitkän aikaa omalakisen kehittäjäyhteisön hallinnan alla. (Zittrain 2008, 2, 27–28.) 1980-luvulle tultaessa internetin suosio oli kasvanut jo niin suureksi, ettei yhteisö enää pystynyt hallinnoimaan verkkoa yksin. Internetin perustoiminnot yksityistettiin 1990-luvulla (Naughton 2016b, 12–16), minkä seurauksena uudet tahot pääsivät kehittämään ja innovoimaan internetiä. Tämä teki siitä demokraattisemman, kun tavalliset kansalaiset pääsivät osallisiksi uudesta teknologiasta (Singer & Friedman 2014, 18–20), mutta myös hajanaisemman ja haavoittuvamman, kun sen hallinnointiin alkoi osallistua hyvin erilaisia ja eri intressejä edustavia toimijoita.

Internetin laajeneva ja avautuva kehitys koski enimmäkseen kuitenkin vain Eurooppaa ja Pohjois-Amerikkaa: kun lännessä nautittiin vapaasta internetistä ja pidettiin sitä demokratian jatkeena, idässä verkkoon pääsyä rajoitettiin ja sen sisältöä sensuroitiin. Internetin historiassa poliittiset vaikutukset näkyvät monella tasolla, myös itse infrastruktuurissa. Valtioilla on edelleenkin laajat oikeudet päättää maansa rajojen sisällä tapahtuvasta viestiliikenteestä, ja koska valtio ylläpitää internet-infrastruktuuria, se voi sulkea koko toiminnan ”vetämällä töpselin seinästä”, kuten esimerkiksi Kiinassa ja Egyptissä on aiemmin tapahtunut (Thompson 2011), ja vuonna 2017 Togossa (Koutonin 2017). Valtiot ovat perustelleet internetin rajoittamista muun muassa nationalismilla, uskonnolla tai taloudella, ja julkishallinto voi rangaistusten uhalla luoda pelon ilmapiirin, minkä seurauksena kansalaiset rajoittavat itse omaa verkon käyttöään. Joissakin maissa rajoitettu internet toimii lisäksi valtion omana propagandavälineenä. (Curran 2012, 49–50.)

Yksityistämisen myötä internetillä ei ollut yhtä ainoaa hallinnoijaa, vaan sen perusarkkitehtuuri oli jaettu usean eri toimijan kesken. Koska toimijoiden joukossa on niin julkisia kuin yksityisiäkin organisaatioita, konsensuksen muodostamisesta internetin kehittämiseksi tuli käytännössä mahdotonta. Kuka tahansa pystyi lisäämään verkkoon omia sovelluksia tai ohjelmiaan, mikä osaltaan laukaisi sen, että joukkoon päätyi paljon myös kyseenalaista koodia. (Zittrain 2008, 28, 30.) Toisin sanoen internet avautui viruksille, vakoilu- ja haittaohjelmille, joiden määrä on nykyisin lukematon. Internetin ja sen infrastruktuurin avoimuus ja demokraattisuus ovat siis osaltaan mahdollistaneet nykyisen, kyberhyökkäyksille alttiin verkkoympäristön.

Rikollisuus, vakoilu ja sota kyberuhkina

Kybermaailman uhat ovat yhä enenevässä määrin osa tavallisen internetkäyttäjän arkea. Arkisia uhkia ovat esimerkiksi kyberhäirintä (*cyber harassment*) (Salter & Bryden 2009, 99) ja kyberkiusaaminen (*cyber bullying*) (von Solms & van Niekerk 2013, 99), jotka voivat ilmetä esimerkiksi asiattomina tai uhkaavina kommentteina sosiaalisessa mediassa. Iso rakenteellinen ongelma on käyttäjien heiveröinen ymmärrys

kybertoimintaympäristöstä ylipäätään (Singer & Friedman 2014, 249), mikä johtaa huijausviestien liitteiden klikkaamiseen tai heikon salasanan luomiseen. Informaation leviäminen ihmisten välityksellä voi aiheuttaa vakavia ongelmia niin yrityksille kuin yksityishenkilöillekin. Perinteisten virusten, haittaohjelmien ja identiteettivarkauksien lisäksi kybertoimintaympäristö on jatkuvasti alttiina muun muassa luonnonkatastrofeille, fyysisen maailman ongelmille (mm. sähkökatkokset, pöly) ja kyberrikollisten hyökkäyksille. Valtioiden harjoittama tiedustelutoiminta, kybervakoilu, on yleistä, ja useat maat suunnittelevat vastaiskuja niitä vastaan kohdistettuihin kyberhyökkäyksiin. Kybersotakin on mahdollinen.

Kyberuhkaksi voidaan yleisellä tasolla nimittää pahantahtoista tarkoitusta vahingoittaa tai tuhota tietoverkkoa, tietojärjestelmää tai päätelaitetta (Lehto ym. 2017, 12). Kyberuhkien jaottelu ei ole vielä vakiintunut, mutta esimerkiksi Suomen kyberuhkamallissa ne on jaoteltu seuraavasti: 1) kyberaktivismi (kybervandalismi, haktivismi), 2) kyberrikollisuus, 3) kybervakoilu, 4) kyberterrorismi ja kyberoperaatiot sekä 5) painostus, sotaa alempi konflikti tai sotaan liittyvä kyberoperaatio (Suomen kyberturvallisuusstrategia 2013). Laajemman tason jaottelu käsittää yleensä **rikollisuuden**, **vakoilun** ja **sodankäynnin** (McGraw 2013: 110). Tässä artikkelissa pureudumme tarkemmin näihin kolmeen ylätason kategoriaan, sillä juuri ne ovat toistuvasti esillä niin tutkimuskirjallisuudessa kuin valtioiden kyberturvallisuusstrategioissakin.

Kyberrikollisuus on kybertoimintaympäristön uhkista yleisimpiä, sillä se näkyy jokaisen internetin käyttäjän arjessa konkreettisella tavalla. Limnéll ym. (2014, 119–120) määrittelevät kyberrikoksen olevan ”tapahtuma, jossa tietokoneet ja/tai -verkot ovat rikollisen toiminnan välineitä, kohteita tai rikoksen tekemisen paikka”. Kybermaailman asiantuntija Mark Johnsonin (2013) mukaan kyberrikoksessa käytetyn tietokoneen tulee lisäksi olla yhteydessä internetiin tai muuhun vastaavaan verkkoon. Valtaosassa kyberrikoksista taustalla on taloudellinen motiivi. Kyberrikollisuuden globaaleja kustannuksia on lähes mahdotonta mitata, sillä seuraukset ovat usein aineettomia. Arvioiden mukaan summa liikkuu jossakin 300 miljardin ja triljoonan dollarin välillä. (Limnéll ym. 2014, 126–127.) Kyberrikollisuus on suuren luokan liiketoimintaa niin taloudellisten vaikutustensa kuin monistettavuutensakin vuoksi. Kyberrikoksia tehtailee joukko alan yrityksiä, jotka myyvät verkossa valmiita viruksia tai palvelinestohyökkäyksiä. Toimintaa rahoittavat paitsi yksityishenkilöt myös tietyt valtiot, jotka kokevat kyberrikokset keinona puolustautua muiden valtioiden kyberhyökkäyksiä vastaan. (Singer & Friedman 2013, 90.) Kyberrikollisuutta onkin vaikea saada kuriin, kun lakia valvova valtiovalta on siinä epäsuorasti mukana.

Kyberrikokset luokitellaan useaan eri kategoriaan: 1) tietoa ja tietojärjestelmiä vastaan tehdyt hyökkäykset, 2) tietokoneita hyödyntävät rikokset, 3) sisällöltään rikolliset toimet (esimerkiksi lapsipornografia, rasismi tai vihapuhe) ja 4) kopiosuojaa tai tuotemerkkiä loukkaavat rikokset (Limnéll ym. 2014, 125). Sen lisäksi, että kyberrikokset luokitellaan rikoksen tavoitteen mukaan, niitä voidaan tarkastella myös tavoitteiden saavuttamiseksi käytettyjen keinojen kautta (ks. Taulukko 1). Näitä keinoja on enemmänkin kuin taulukkoon on koottu, eikä mikään menetelmä yleisesti ottaen toimi sellaisenaan. Esimerkiksi bottiverkkoja käytetään usein palvelunestohyökkäyk-

sen toteuttamiseksi, sillä valtava tietokoneverkko voidaan yhdellä komennolla saada lähettämään palvelinpyyntöä jollekin sivustolle. Rikollisille tämä on vaivattomampaa kuin pyytää yksittäisiä ihmisiä siirtymään sivustolle samanaikaisesti palvelun kaatamiseksi. Ajanmukaisia tilastoja tällaisten moniulotteisten kyberhyökkäysten yleisyydestä on kuitenkin erittäin vaikea löytää.

Taulukko 1. Yleisimmät kyberrikollisuuden menetelmät (Johnson 2013)

Menetelmä	Kuvaus
Hakkerointi (*Hacking*)	Murtautuminen tietokonejärjestelmiin ja tietoverkkoihin manuaalisesti hakkerin omia kykyjä hyödyntämällä.
Tunkeutuminen (*Code Injection*)	Koodin syöttäminen tietokoneohjelmaan niin, että sen alkuperäistä toimintoa häiritään.
Cross site scripting (XXS)	Verkkosivuston linkittäminen haittaohjelman sisältävän sivun yhteyteen, jolloin alkuperäinen sivusto saastuu.
Mies välissä -hyökkäys (*Man-in-the-middle*)	Tapahtuma, jossa hyökkääjä asettuu kahden osapuolen väliin tarkoituksenaan häiritä niiden välistä kommunikaatiota.
Vakoiluohjelma (*Spyware*)	Ohjelma, jolla kerätään henkilökohtaista tietoa, kuten sisäänkirjautumistietoja, tietokoneen käyttäjästä.
Troijalaiset, madot, virukset (*Trojans, worms, viruses*)	Haittaohjelmia, jotka välittävät tietoa tai häiritsevät ohjelman käyttöä tai jopa vahingoittavat tietoverkkojärjestelmää.
Palvelunestohyökkäys (*DoS attacks*)	Hyökkäyksen tarkoituksena on kaataa valikoidut palvelimet tai verkot ylikuormittamalla sivusto palvelinpyynnöillä.
Bottiverkko (*Botnet*)	Tuhansista tai jopa miljoonista tietokoneista koostuva verkko, joka valjastetaan rikollisen toiminnan käyttöön.

Tietoverkkojen erityisominaisuuksia ja haavoittuvuuksia hyväksi käyttävien varsinaisten kyberrikosten lisäksi valtiollinen tiedustelutoiminta ja jopa suoranainen **vakoilu** näyttävät kuuluvan olennaisena osana kybertoimintaympäristöjen rakentumiseen. Tiedustelemalla hankittua tietoa on käytetty vallan välineenä läpi ihmiskunnan historian. Esimerkiksi sotatoimissa on välttämätöntä tuntea vastapuolen taktiikat ja joukkojen fyysinen sijoittuminen. Kun tiedustelua aletaan harjoittaa laittomin keinoin, siitä tulee vakoilua. Limnéll ym. (2014, 129) kirjoittavat, että kyberaikakausi on mullistanut vakoilun mahdollisuudet. Ennen tieto oli fyysisessä muodossa ja vakoilijan oli fyysisesti mentävä sinne, missä tieto sijaitsi. Nykyään digitalisoituun tietoon

voidaan päästä käsiksi toiselta puolelta maailmaa tietovarastojen ollessa yhteydessä verkkoon.

Tieto- ja viestiliikenteen tutkija Herbert S. Lin (2010, 63) määrittelee kybervakoilun olevan "toimintoja ja operaatioita – mahdollisesti pitkälle aikavälille sijoitettuna –, joiden avulla hankitaan luottamukselliseksi tarkoitettua tietoa ja joiden on tarkoitus säilyä tai levitä vastapuolen tietokoneissa ja tietoverkoissa". Linin mukaan kybervakoilu on ei-tuhoava kyberuhka, kun taas kyberhyökkäysten tarkoitusperät ovat tuhoavia. Vakoilun tarkoituksena on hankkia tietoa, mutta kyberisku tavoittelee jonkin tietojärjestelmän, ohjelman tai muun "kybertuhoamista". (Lin 2010.) Lisäksi vakoilulle on olennaista, että sillä on yleensä jokin taloudellinen, poliittinen tai sotilaallinen päämäärä. Sen vuoksi todennäköisimmät kybervakoilun toimijat ja kohteet ovat yrityksiä ja valtioita (Limnéll ym. 2014, 129–130).

Kiinan ja Yhdysvaltojen toisiinsa kohdistuvia syytöksiä ei voida ohittaa puhuttaessa kybervakoilusta. Moni tutkija mainitsee nämä maat maailman suurimmiksi kybervakoilun harjoittajiksi (ks. esim. Jantunen 2010; Limnéll ym. 2014, 130; Pelican 2012; Singer & Friedman 2013, 92). Vuonna 2009 tutkijat löysivät internetissä levinneen verkoston, joka yhdisti toisiinsa 1 295 palvelinta 103:ssa eri maassa. GhostNetiksi nimetty vakoiluverkosto oli levinnyt muun muassa suurlähetystöihin ja ulkoministeriöihin sähköpostin liitetiedoston välityksellä. Verkoston alkuperä paikannettiin Kiinaan. (Singer & Friedman 2013, 93.) Kenties maailman tunnetuin tiedustelurikos on Edward Snowdenin tapaus, jossa Snowden ei tosin itse ollut vakoilijan asemassa vaan hän paljasti Yhdysvaltojen pitkään jatkuneen systemaattisen kybervakoilun tuloksia. Kyseinen tapahtuma osoittaa, että fyysinen vakoilu ei ole katoamassa minnekään – siitä on tullut vain entistä moniulotteisempaa ja kekseliäämpää (Limnéll ym. 2014, 129; Kubitschko 2015, 79–80).

Myös **kybersodasta** puhutaan paljon poliittisten päättäjien keskuudessa (ks. Lawson 2012). Vaikka vain pienen osan kyberhyökkäyksistä katsotaan edustavan sotatoimia, kybersodalle annetaan puolustusstrategioita mietittäessä suuri merkitys. Monet tutkijat katsovat, että poliittisesta painoarvostaan huolimatta kybersodasta puhutaan liian heppoisin perustein, mikä osaltaan johtuu siitä, ettei käsitettä ole määritelty riittävän selkeästi (Limnéll ym. 2014, 138–139). Singerin ja Friedmanin (2014, 121) mukaan hyökkäyksen määrittely kybersodaksi vaatii todellisen fyysisen seurauksen: kuolemantapauksia, väkivaltaa tai merkittävää fyysistä tuhoa. McGraw (2013, 112) puhuu kineettisestä vaikutuksesta tarkoittaessaan samaa asiaa. Valtiot esimerkiksi vakoilevat toisiaan jatkuvasti ja jäävät siitä kiinni, mutta yksikään valtio ei ole aloittanut sotatoimia varastettujen tiedostojen vuoksi. Sodankäynnin fyysinen ehto jääkin kybersodan osalta usein täyttymättä.

Kybermaailma tarjoaa sodankäyntiin uuden operatiivisen ulottuvuuden, mikä mahdollistaa sotatoimien aloittamisen digitaalisella hyökkäyksellä ilmaiskujen sijasta. Kyberhyökkäykset ovat samalla tavalla poliittisen vallankäytön ja painostamisen välineitä kuin fyysisestikin toteutettavat sodankäynnin operaatiot. Moni länsimainen valtio onkin nostanut kyberulottuvuuden osaksi puolustusstrategiaansa perinteisten sodankäynnin ulottuvuuksien – maan, meren, ilman ja avaruuden – rinnalle. Kyber-

ulottuvuus on muille ulottuvuuksille rinnasteinen, mutta myös osa niitä. Lähes kaikkiin sotatoimiin liittyy nykyisin jokin kyberkomponentti, kuten miehittämättömät lennokit tai joukkojen koordinointi digitaalisten järjestelmien avulla. (Limnéll ym. 2014, 140–142.)

Kybertoimintaympäristö on tuonut osaksi sodankäynnin muotoja myös informaatiosodankäynnin, johon liittyviin käytännön esimerkkeihin paneudumme tarkemmin tämän artikkelin loppupuolella. Puolustusministeriön selonteossa informaatiosodankäynti määritellään tiedolla vaikuttamiseksi ja siltä suojautumiseksi valtion yhteiskunnallisessa ja sotilaallisessa päätöksenteossa (Valtioneuvoston kanslia 2004, 156). Kyse on siis siitä, miten informaatiota hyödynnetään strategisesti eri informaatiokanavissa kohteen psykologisen ja henkisen tasapainon häiritsemiseksi (Limnéll ym. 2014, 148). Käytännössä informaatiosodankäyntinä voidaan tarkastella myös tietoon tai mielipiteisiin kohdistuvia vaikutusyrityksiä niin perinteisessä kuin sosiaalisessakin mediassa, eli vanhanaikaisesti ilmaistuna propagandaa (ks. Jantunen 2015, 17–19). Informaatiosodankäynti on usein keskeinen osa nykyisiä kybersodankäynnin muotoja.

Kybersodankäynnin tunnetuimpia esimerkkejä ovat Venäjän hyökkäys Georgiaan vuonna 2008 ja Stuxnet-vakoiluohjelma, jonka Yhdysvallat syötti Iranin tietojärjestelmään. Vuoden 2008 konfliktissa Venäjä puuttui maan sisäisiin ongelmiin ja lähetti omat joukkonsa Georgian rajojen yli päivä sen jälkeen, kun maan tietoverkot oli ensin kaadettu palvelunestohyökkäyksellä. Tutkijat eivät ole pystyneet osoittamaan, että Venäjä olisi ollut iskun takana, mutta laajan kansainvälisen uutisoinnin myötä kyberhyökkäys on laitettu Venäjän nimiin (Tikk ym. 2008, 4, 12). Georgian ja Venäjän konfliktissa voidaan puhua kybersodasta, sillä ensin maan tietoverkot kaadettiin, minkä jälkeen fyysiset asevoimat marssivat laittomasti toisen valtion alueelle sotatoimiin. Lähtökohdat ovat siis olleet kybermaailmassa, minkä lisäksi fyysisen seurauksen ehto on toteutunut (esim. Jantunen 2015, 28–31).

Stuxnet ei aiheuttanut sotatoimia, mutta on hyvä esimerkki kyberaseesta toisen osapuolen kehityksen viivästyttäjänä. Stuxnet oli vuonna 2010 löydetty haittaohjelma, joka aiheutti takaiskun Iranin ydinaseohjelmalle. Haittaohjelma sai uraanin rikastamisessa käytettävät sentrifugit pyörimään väärällä nopeudella, vaikka niitä kontrolloivat ohjauslaitteet näyttivät oikeita arvoja. Lopputuloksena oli vioittuneita sentrifugeja ja käyttökelvotonta uraania. (McGraw 2013, 112, 115.) Sen lisäksi, että Stuxnet hidasti Iranin ydinaseohjelmaa, se oli suhteellisen edullinen toteuttaa. Stuxnetin hinnaksi arvioidaan 10 miljoonaa dollaria, kun taas hävittäjälentokone maksaa valtiolle jopa kymmenen kertaa enemmän (Limnéll ym. 2014, 140).

Yhteenvetona voidaan todeta, että kyberuhkilla on omat erityispiirteensä, mutta samalla ne myös linkittyvät toisiinsa, ja niitä täytyy usein käytännössä ajatella yhtenä, moniulotteisena kokonaisuutena eli hybridinä. Kybervakoilu on rikollista toimintaa, erilaisten laitteiden häirintä poliittisin päämäärin voidaan katsoa sotatoimiksi, ja toisaalta kybersodassa pyritään hankkimaan tietoa vastapuolen toimista erilaisin vakoiluohjelmin. Vakoilu eroaa rikollisuudesta ja sodasta siinä, että se ei itsessään pyri tuhoamaan vaan hankkimaan tietoa. Vakoilun keinoin hankittua tietoa voidaan kuitenkin käyttää tuhoamisen välineenä. Uhkiin vastaaminen jää käytännössä valtion

tehtäväksi, sillä sen vastuulla on säätää lakeja, joissa rikokset määritellään, sekä ylläpitää oikeuslaitosta, joka huolehtii siitä, että rikollisesta toiminnasta saa asiaan kuuluvan rangaistuksen.

Valtio kybermaailman toimijana

Valtio on olennainen osa kybertoimintaympäristöä, sillä sen täytyy pystyä suojaamaan oma digitaalinen infrastruktuurinsa, yhteiskunnan elintärkeät tehtävät ja kansalaisten tarvitsemat elämisen mahdollistavat palvelut (Singer & Friedman 2014, 197). Lisäksi valtio on vastuussa kokonaisturvallisuudesta ja laeista, joilla kybertoimintaympäristöä säädellään, kuten tässäkin artikkelissa on jo yksityisyyden suojan osalta todettu (Puolustusministeriö 2017a). Kokonaisturvallisuus on määritelty tilaksi, jossa yhteiskunnan elintärkeisiin toimintoihin kohdistuviin uhkiin ja riskeihin on varauduttu (Sanastokeskus 2017, 16). Internetin yksityistyttyä valtio on pyrkinyt pysyttelemään mukana teknologisessa kehityksessä, mikä on johtanut siihen, että valtaosa valtionhallinnon asiakirjoista, viestinnästä ja päätöksenteosta tapahtuu verkossa. Lisäksi valtion rajojen sisäpuolella on vesi- ja sähkölaitoksia, liikennettä ja maanviljelyä, jotka kaikki ovat jollakin tavalla yhteydessä verkkoon. Valtio on tahtomattaankin osa kybertoimintaympäristöä, eikä sen vuoksi voi toimia siellä ilman strategista suunnitelmaa (Shackelford & Craig 2014).

Kybertoimintaympäristössä vaikuttaminen ei kuitenkaan ole valtiolle helppoa. Siihen sisältyy ainakin kolmenlaisia haasteita. Ensinnäkin valtio ylläpitää byrokratiaa ja on siksi hidas (Singer & Friedman 2014, 198), eikä se pysty kovin helposti vastaamaan kybermaailman nopeuteen, jossa hyökkäykset tapahtuvat ilman ennakkovaroituksia. Fyysisessä maailmassa käytössä olevat keinot, joilla toimintoja jäljitetään, eivät välttämättä toimi kybermaailmassa (Choucri, Madnick & Ferwerda 2014, 98). Tämän vuoksi isojen strategisten päätösten tekeminen ja lakimuutokset vievät aikaa, ja kun ne lopulta valmistuvat, niiden sisältö on ehkä jo ehtinyt vanhentua.

Toisekseen valtio joutuu jatkuvasti pohtimaan puolustuspolitiikkaansa ja kansainvälisen yhteistyön mahdollisuuksia muuttuvassa digitaalisessa ympäristössä. Perinteiseen puolustukseen verrattuna toimiva kyberturvallisuus vaatii yhteistyötä niin kansallisella, kahdenvälisellä kuin globaalillakin tasolla (Choucri ym. 2014, 104). Fyysisessä maailmassa on paljon yksinkertaisempaa osoittaa maiden väliset rajat ja niitä puolustavat sotavoimat. Valtiot pystyvät esimerkiksi asettamaan toisensa kauppasaartoon tai muihin pakotteisiin, jos suvereniteetti on uhattuna. Kybermaailmassa vastustajaa ei kuitenkaan aina tunneta, tai hyökkäyksen taustalla on jokin muu toimija kuin valtio. Kyberrikollisuus ei myöskään pysyttele maiden rajojen sisäpuolella, mikä tekee siitä valtioille yhteisen uhkan ja rangaistusten asettaminen vaikeutuu.

Kansainvälinen yhteistyö ei myöskään jakaudu tasa-arvoisesti maiden kesken. Ellada Gamreklidzen (2014, 203–204, 214) mukaan kyberturvallisuusyhteistyötä vaikeuttaa digitaalinen kuilu, jolla tarkoitetaan perinteisesti ihmisten, yritysten ja maantieteellisten alueiden välistä kahtiajakoa tieto-ja viestintäteknologiasta hyötyjiin ja

sen kehityksen ulkopuolelle pudonneisiin. Valtioilla, joilla ei ole kattavaa tietoverkkoinfrastruktuuria, ei ole myöskään keinoja puolustautua kyberhyökkäyksiä vastaan. Näiltä valtioilta puuttuvat kyberturvallisuusstrategiat, hallinnolliset elimet ja asiantuntevat ihmiset, jotka voisivat edistää kyberturvallisuutta. Rajallinen tietoverkkoinfrastruktuuri ei kuitenkaan poista sitä tosiasiaa, että näissä maissa kyberhyökkäykset kohdistuvat valtion kriittisimpään tietoliikenteeseen, kuten teollisuuskäyttöön tarkoitettuun SCADA-kontrollijärjestelmään ja pankkien järjestelmiin.

Oletettavaa on, että yhteistyö vasta kehittyvien ja jo kehittyneiden kybervaltioiden välillä on melko vähäistä, sillä kehittyvillä valtioilla ei ole juurikaan annettavaa vastapuolelle (Sabillon, Cavaller & Cano 2016, 79). Vaikka kansainvälisestä yhteistyöstä puhutaan paljon, kybermaailmasta puuttuvat kansainväliset standardit, joiden puitteissa kyberturvallisuutta toteutetaan. Lisäksi maakohtaiset lainsäädännöt poikkeavat toisistaan, mutta sen sijaan, että ne yhtenäistettäisiin, Sabillon ym. (2016) ehdottavat, että kybertoimintaympäristöille luotaisiin oma kansainvälinen lakinsa. Globaalin standardin ja lainsäädännön luominen vaatii heidän mukaansa kehittyneiden maiden panosta, jotta myös kehittyvät maat pääsisivät kiinni kyberaikakauteen.

Kolmas ja viimeinen valtion haaste kybertoimintaympäristön toimijana on kysymys valtion oikeudesta määrätä yksityisen sektorin toiminnasta. Kybertoimintaympäristön perusarkkitehtuuria ylläpitävät ei-hallinnolliset elimet, eivät valtiot (Choucri ym. 2014, 98). Internet Engineering Task Force (IETF) on alkujaan vapaaehtoisista koostunut insinööri- ja tiedeyhteisö, joka kehittää internet-standardia ja -protokollia. IETF:n toiminnalle teknistä tukea antaa Internet Engineering Steering Group (IESG), joka taas on yhteistyössä Internet Architecture Boardin (IAB) kanssa. Nämä vastaavat toiminnastaan Internet Societylle (ISOC), joka on perustettu valvomaan avoimen lähdekoodin laillisia oikeuksia. Lisäksi internetissä on muitakin sen toiminnan kannalta oleellisia osia, kuten nimipalvelu, jota pyörittää Internet Corporation for Assigned Names and Numbers (ICANN). ICANN jakaa ja hallinnoi verkkosivujen IP-osoitteita. (Singer & Friedman 2014, 27–29.)

Edellä esitellyt organisaatiot ovat olemassa, jotta internet toimisi. Turvallisuudesta vastaamaan on lisäksi perustettu CERTejä (Computer Emergency Response Teams). CERT-toiminnot on kehitetty kansainvälisessä yhteistyössä, mutta ne eivät kuitenkaan ole valtiohallinnon alaisia organisaatioita. CERTien tehtävä on ehkäistä kyberhyökkäyksiä, suositella turvallisimpia teknologioita ja varmistaa verkon jatkuvuus. Sen lisäksi, että on olemassa kansainvälinen niin sanottu globaali CERT, jokaisella maalla on omansa (esimerkiksi Suomella CERT-FI). CERTit ovat jakautuneet alueellisesti, mutta myös sillä perusteella, ketä ne on perustettu suojelemaan (mm. yliopisto, yksityinen sektori, pankkiviestintä) ja minkälaista uhkaa ne torjuvat (mm. virukset, vakoiluohjelmat, madot). (Choucri ym. 2014, 104–105.)

Kysymys kybertoimintaympäristön hallinnoijasta ei siis ole yksiselitteinen. Tutkijat pohtivat sitä, onko valtiolla oikeus määrätä kybertoimintaympäristöstä, jos ne eivät ole sen varsinaisia ylläpitäjiä. Muun muassa turvallisuus- ja tietotekniikan tutkija Julian Richards (2014, 61) kyseenalaistaa valtion oikeuden säätää yrityksiä velvoittavia lakeja. Limnéllin ym. (2014, 46) mukaan valtio saa ohjeistaa yksityistä sektoria, mutta

kybertoimintaympäristön turvaaminen ilman läheistä yhteistyötä yritysten kanssa ei ole mahdollista. Loppujen lopuksi valtaosa valtioiden kybermääräyksistä ja -säädöksistä kuitenkin koskee yksityistä sektoria. Richardsin (2014, 68) mukaan laajamittaisesta kyberrikollisuudesta rankaiseminen kuuluu kansainväliselle tuomioistuimelle. Silti valtiot pyrkivät kyberturvallisuusstrategioidensa mukaan kitkemään rikollisuuden itse. Ongelmana on, että strategiat on pääpiirteissään kehitetty kybersotia tai -terrorismia vastaan, ei niinkään rikollisuutta. Lisäksi valtiot voivat itse olla kyberhyökkäysten tai muun kyberrikollisuuden takana. Kybertoimintaympäristöstä päättäminen ei voi olla pelkästään yksityisenkään sektorin tehtävä.

Haasteiden ja uhkien ohella kybertoimintaympäristö tarjoaa myös mahdollisuuksia. Se, kuinka valtiot onnistuvat hyödyntämään muun muassa niin sanottua big dataa, pilvilaskentaa (*cloud computing*) ja esineiden internetiä (*internet of things*), on merkittävä kansallinen kilpailuvaltti tulevaisuuden kybermaailmassa (Min, Chai & Han 2015, 13). Kybermaailma on tila, jossa valtio ainakin ihannetapauksessa pystyy kohtaamaan kansalaisensa ja muodostamaan realistisen kuvan heidän tarpeistaan ja oikeuksistaan, ja näin palveluiden personointi tekee asioinnista viiveettömämpää (Sabillon, Cavaller & Cano 2016, 67). On kuitenkin valtiosta itsestään kiinni, kuinka hyvin se tuntee omat resurssinsa ja onnistuu sisällyttämään ne kyberturvallisuusstrategiaansa.

Kyberstrategiat valtiollisina työvälineinä

Kyberturvallisuusstrategia on valtion turvallisuussuunnitelma kybertoimintaympäristöä varten ja olennainen osa valtion uskottavuutta ja luotettavuutta (ks. Limnéll ym. 2014, 59, 158). Strategian tarkoitus on kartoittaa kybertoimintaympäristön tarjoamia pitkän aikavälin mahdollisuuksia riskit huomioiden. Mitä suuremmat ovat visiot eli mitä enemmän valtio näkee kybertoimintaympäristössä mahdollisuuksia, sitä laaja-alaisemmiksi kasvavat myös riskit. (Limnéll ym. 2014, 157–158.) Strateginen toimintamalli on kuitenkin valtion kyberturvallisuuden elinehto (Gamreklidze 2014, 204). Siksi myös strategian toteutumista seurataan aktiivisesti. Esimerkiksi Suomessa julkaistiin äskettäin kyberturvallisuuden tavoitetilaa ja sen saavuttamista käsittelevä tutkimus (Lehto ym. 2017), jossa analysoitiin turvallisuustilannetta yleisellä tasolla sekä selvitettiin Suomen kyberturvallisuuden nykytilaa ja sen kehittämistarpeita julkisella ja yksityisellä sektorilla.

Jo lähes 80 valtiota on julkistanut ensimmäisen tai päivitetyn version maansa kyberturvallisuusstrategiasta 2010-luvulla (CCDCOE 2016). Moni strategioista on julkaistu vuoden 2013 jälkeen, jolloin sattui yksi historian merkittävimmistä tietovuodoista, kun Yhdysvaltain entinen tiedustelutyöntekijä Edward Snowden paljasti maan tiedustelupalvelu NSA:n laajamittaisen kuuntelu- ja seurantaohjelman (Gellman, Blake & Miller 2013). Nämä tapahtumat eivät ole ainakaan vähentäneet valtioiden kasvavaa kiinnostusta kyberturvallisuuteen. Kyberturvallisuuden hahmottaminen nimenomaan valtioiden tuottamien dokumenttien kautta on loogista: kybermaailman merkittävinä mutta kiistanalaisina toimijoina niiden suunnittelemat strategiset toimenpiteet, lain-

säädäntö ja virallisesti käyttöön ottamat termit vaikuttavat epäsuorasti jokaisen kansalaisen verkon käyttöön.

Kyberturvallisuusstrategian julkaisseet valtiot perustelevat tarvetta strategialle niin tiedon kuin kansalaisten fyysisen turvallisuuden näkökulmasta. Usein turvallisuutta ylläpidetään hallitsemalla eli olemalla tietoisia muiden kybermaailman toimijoiden liikkeistä. Tämä edellyttää tiedustelua. Ongelmalliseksi tiedustelu voi muuttua silloin, jos kerättyä dataa ei kyetä turvaamaan tai säilyttämään oikealla tavalla, tai jos kyberturvallisuuden kustannuksella pyritään rajoittamaan tai valvomaan kansalaisia. (Limnéll ym. 2014, 60.) Esimerkiksi keskustelua herättäneessä autoverolakiuudistuksessa vuonna 2017 autoihin kaavailtiin asennettavaksi ”musta laatikko”, joka keräisi ajokilometrit talteen. Päinvastaisista vakuutteluista huolimatta sen suojauksen todettiin olevan hyökkääjille helposti läpäistävä ja näin ollen uhka kansalaisten yksityisyydensuojalle (esim. Mansikka 2017). Tiedustelun lisäksi dataa, erityisesti metadataa, kerätään kansalaisista myös sosiaalisen median palveluista. Samaan tapaan kuin yksityiset toimijat, valtio perustelee tätä paremmilla yhteisillä palveluilla ja turvallisuuden takaamisella (van Dijck 2014).

Sabillon ym. (2016, 79) ovat luoneet kansallisen kyberstrategiamallin, joka perustuu Kansainvälisen televiestintäliiton (*International Telecommunication Union*), Naton, OECD:n ja EU:n suosituksiin. Sabillonin ym. mukaan paras mahdollinen kyberstrategia saavutetaan, kun valtio on tietoinen resursseistaan strategian toteuttamiseksi, onnistuu toteuttamaan suunnitelmansa käytännön tasolla ja lisäksi pyrkii kehittämään ja parantamaan toimintaansa entisestään. Mallin mukaan strategian tulee nojata kyberkulttuuriin, joka on kaiken kybertoiminnan pohja ja jota vahvistetaan osana koulutusjärjestelmää. Valtion panos strategiaan määrittää sidosryhmät, suorituskyvyn ja kansainvälisen yhteistyön. Lisäksi onnistuneen strategian kannalta on olennaista, kuinka valtio tekee yhteistyötä kyberyhteisön kanssa, onnistuu kehittämään lainsäädäntöään, järjestää hallinnolliset ja organisatoriset elimet sekä kyberpuolustuksen. Lopputulemana on kyberturvallisuusstrategia, joka mahdollistaa nopean palautumisen kyberhyökkäyksistä, vahvan kyberpuolustuksen ja tietoisuuden sekä kehittää valtion kybertoimintaa entisestään.

Sabillonin ym. (2016) mallista löytyvät melko pitkälle samat asiat, jotka Limnéll ym. ovat löytäneet jo olemassa olevista strategioista. Yleisimmät kyberturvallisuusstrategioissa esitetyt toimenpiteet ovat 1) poikkihallinnollinen yhteistyö, jossa tieto kulkee hallintoyksiköstä toiseen ja kaikki ymmärtävät kokonaisturvallisuuden merkityksen, 2) kyberiskujen ennaltaehkäisy ja proaktiivinen toiminta, 3) kansainvälinen yhteistyö, 4) lainsäädännön saattaminen vastaamaan teknologista kehitystä, 5) tutkimus- ja kehittämistyö, 6) ensisijaisten kohteiden (kuten infrastruktuuri) turvaaminen sekä 7) kyberturvallisuuskeskuksen ja vastaavan poliittisen elimen perustaminen. (Limnéll ym. 2014, 84.) Valtion poliittinen, sotilaallinen ja maantieteellinen asema vaikuttavat siihen, miten se pystyy näitä toimenpiteitä toteuttamaan ja millaisiin uhkiin vastaamaan. Jos valtiolla ei ole resursseja, myös mahdollisuudet pysyvät pienimuotoisina. Sen sijaan johtavat kybervaltiot, kuten Yhdysvallat tai Iso-Britannia, pystyvät visioimaan strategioissaan laajempia kokonaisuuksia ja globaalin tason toimijuutta.

Valtiot myös ottavat kyberturvallisuusstrategioita luodessaan oppia toisiltaan. Kuten olemme todenneet, kybermaailma on vielä uusi ja varsin tuntematon asia. Vaikka valtiot olisivat kiinnostuneita kyberturvallisuudesta, se ei vielä tarkoita, että ne todella tuntisivat sitä. Esimerkiksi maa, joka ei ole koskaan joutunut kyberhyökkäyksen kohteeksi, ei osaa arvioida omaa toimintakykyään iskun sattuessa yhtä hyvin kuin maa, joka on joutunut sellaista vastaan puolustautumaan. Samasta syystä strategioissa toistuu epäjohdonmukaisuus tietoturvan ja kyberturvallisuuden käsitteiden käytössä, eli niitä saatetaan käyttää toistensa synonyymeina (von Solms & van Niekerk 2013, 97). Niiden eroa ei välttämättä osata selittää, koska kybermaailmaa ei vielä ymmärretä.

Kansalliset kyberturvallisuusstrategiat ovat valtiolähtöisesti tuotettuja tekstejä, joissa luodaan toinen toistaan suurempia visioita vahvasta ja luottamusta herättävästä ”kybervaltiosta”. Niiden ensisijainen tehtävä on vahvistaa valtioiden välistä talous- ja puolustuspoliittista yhteistyötä. Tavallisia internetin käyttäjiä strategiat eivät juuri tavoita tai kiinnosta; vain kaksi strategiaa on herättänyt julkaisuajankohtanaan keskustelua kotimaansa mediassa. (Jansson 2017, 86–87, 89.) Tästä huolimatta Pällin ym. (2009, 309) mukaan strategiatekstit on kirjoitettu niitä työstäneiden ja työssään tarvitsevien lisäksi laajalle sidosryhmäjoukolle, johon lukeutuvat muun muassa asukkaat, kansalaiset, turistit sekä muut samanarvoiset toimijat eli muut valtiot ja tiedotusvälineet. Strategiateksti on siis paitsi valtion sisäinen työväline, myös keino esitellä toimintaa muille ja saada muut vakuuttuneeksi valtion toimintakyvystä ongelmien sattuessa kohdalle.

Juuri tästä syystä kansalliset strategiat ovat yleisesti nähtävillä, vaikka niissä käsitellään puolustuspoliittisia yksityiskohtia ja esitellään fyysisten voimakeinojen käyttöä esimerkiksi kybersodan uhatessa (Richards 2014, 63). Strategioissa identifioidut uhkat ja vaarat toimivat pontimena sille, että valtio voi yksityiskohtaisesti esitellä, miten hyvin se on niihin varautunut ja miten tehokkaasti se huolehtii kansalaistensa turvallisuudesta. Richardsin (2014, 68) mukaan paras keino puolustautua kyberuhkia vastaan onkin informaation vapaa liikkuvuus. Kybermaailmassa on syytä hyväksyä se, että turvallisuus tulee väistämättä pettämään jossain vaiheessa (Limnéll ym. 2014, 159). Käytännön tasolla kyberturvallisuudesta käytävään julkiseen keskusteluun kuitenkin vaikuttanevat huomattavasti enemmän tiedotusvälineissä julkaistut uutiset kyberuhkista – rikollisuudesta, vakoilusta ja sodankin mahdollisuudesta.

Median merkitys kybertoimintaympäristön rakentumisessa

Kuten olemme tässä artikkelissa esittäneet, kybertoimintaympäristö ja kyberturvallisuus ovat suhteellisen uusia käsitteitä niin valtioille kuin niiden kansalaisillekin. Kyberalkuisten sanojen käyttö on esimerkiksi populaarijulkisuudessa selvästi yleistymässä, mutta käsitteiden käyttö ei sinänsä vielä kerro niiden vakiintuneista tai vakiintumattomista määritelmistä mitään. Monipuolisesta historiastaan huolimatta ”kyber” etuliitteenä tuntuu suomalaisessa julkisuudessa liittyvän nykyisin aivan tietynlaisiin puhetapoihin, jotka näyttäytyvät yhtäältä kiehtovina ja mielikuvitusta stimuloivina, toisaalta

pelkoja ja uhkakuvia herättelevinä (ks. esim. Postila 2017). Kielipankin sanomalehti- ja eduskunta-aineistoista elokuussa 2017 tekemiemme hakujen perusteella kyber-alkuiset sanat liittyvät voittopuolisesti negatiivisiin konteksteihin, kuten uhkan, hyökkäyksen, puolustuksen ja sodan kaltaisiin teemoihin (ks. Eduskunta 2017; Kansalliskirjasto 2011).

Kyber-alkuisiin sanoihin näyttää siis lähes poikkeuksetta liittyvän digitaalinen uhka, mikä sävyttää pitkälti myös niiden esiin nostamaa tai niistä käytyä keskustelua (ks. esim. Rudner 2013). Tämä ”uhan diskurssi” sopii hyvin siihen huomioon, että kyberiskuiksi nimetyt hyökkäykset ovat jo melko tavallisia ja ne nostetaan helposti tärkeiden uutisaiheiden joukkoon. Erityisesti laajat, globaalin tason kyberhyökkäykset on usein strategisesti kohdistettu yritystä, valtiota tai jotakin tiettyä toimintaa vastaan. (Naughton 2016b, 20–21.) On arvioitu, että tulevaisuudessa yhä merkittävämmäksi kasvava uhka liittyy esineiden internetiin (von Solms & van Niekerk 2013, 100). Kun kodinkoneet, elektroniset laitteet ja kulkuvälineet on yhdistetty verkkoon, kyberhyökkäyksiä voidaan toteuttaa laaja-alaisemmin kuin aiemmin. Toisaalta ne voivat olla entistä kohdennetumpia, jopa iskuja yksilöä vastaan. Hyökkäys voi tapahtua esimerkiksi siten, että auton ajotietokoneeseen tunkeudutaan sen ollessa käytössä ja kuljettaja menettää ajoneuvonsa hallinnan. Tämäntyyppisellä pienimuotoisellakin häirinnällä voi olla vakavia seurauksia sekä uhrille että häirikölle – toisaalta on olennaista kysyä, miksi hyökkäys on yleensäkään toteutettu (Singer & Friedman 2014, 38). Jotkut kyberhyökkäykset tapahtuvat siksi, että niiden toteuttaja kykenee iskuun ja etsii huomiota teolleen. Tällöin hyökkäyksestä uutisointi ja sitä seuraava julkinen keskustelu ovat tärkeässä roolissa sen “onnistumisen” kannalta.

Kyberrikoksiin keskittyviä uutisia on viimeksi kuluneen vuoden aikana nähty aiempaa enemmän. Esimerkiksi keväällä 2017 valtavasti julkisuutta sai 12. toukokuuta alkanut maailmanlaajuinen kyberhyökkäys. Yle uutisten mukaan kyseessä oli Microsoftin Windows-käyttöjärjestelmän haavoittuvuutta hyödyntänyt kiristysohjelma (*ransomware*), joka lukitsi yksittäisen käyttäjän kovalevyn sisällön salasanan taakse ja vaati tätä maksamaan 300–600 dollarin lunnaat bitcoineina (Kippo 2017; Kokkonen 2017). Tämä WanaCryptor 2.0 tai WannaCry -nimellä tunnettu hyökkäys vaikutti olevan poikkeuksellisen laaja; jo parin päivän sisällä leviämisestään se teki tuhoja yli 200 000 kohteessa ja 150 maassa ympäri maailman. Maailmanlaajuisesti toimivat yritykset, kuten FedEx ja Telefónica, sekä Britannian kansallinen terveydenhuoltojärjestelmä NHS vaikuttivat hyökkäyksen ensiaallossa olevan pahimmin kärsineiden joukossa (BBC 2017).

Kyberhyökkäysten suuruuden ja hallitsemattoman leviämisen korostaminen kuuluu tyypillisiin keinoihin, joiden kautta uutisissa kuvaillaan niiden toimintaa. Koska yksittäisten iskujen vahingollisuutta on vaikea hahmottaa pelkistä luvuista, tarjotaan lukijoille tulkintojen tueksi usein myös mittakaavaa, jossa muistutetaan aiemmista tunnetuista iskuista ja niiden arvioiduista kokoluokista. Historian toistaiseksi suurimpana paljastuneena tietomurtona pidetään Yahoota vastaan vuosina 2013 ja 2014 tehtyjä hyökkäyksiä, joiden laajuus paljastui vasta vuonna 2016. Iskuissa varastettiin jopa miljardin käyttäjätilin tiedot. (Thielman 2016.) Vuonna 2011 ja 2014 hyökkääjät iskivät Sony PlayStation Networkiin ja varastivat pelaajien luottokorttitietoja (BBC 2014).

Huhtikuussa 2011 alkaneessa hyökkäyksessä jopa 77 miljoonan pelaajan henkilötiedot joutuivat vääriin käsiin (Phillips 2016).

Paneutumista kyberhyökkäysten leviämiseen ja niiden mittakaavaan voi tulkita esimerkiksi siten, että perinteistä journalistista tarkastelukulmaa – keskittymistä tekijöihin ja kokijoihin – on tietoverkkorikollisuudesta kertoviin juttuihin vaikea rakentaa. Esimerkiksi WannaCry:n alkuperä paikannettiin lehtijutuissa epämääräiseen Shadow Brokers -nimiseen hakkeriryhmään, jonka ilmoitettiin edellisenä vuonna varastaneen Yhdysvaltain puolustusvoimien (*National Security Agency*, NSA) varastosta kokoelman ”kyberaseita” (Solon 2016). Toisaalta uutisteksteissä muistutettiin siitä, että WannaCry:n tapaiset kyberuhat perustuvat varsin vanhaan, yksinkertaiseen ja yleisesti tunnettuun tekniikkaan (Jokiniemi 2017). Kyberrikollisten ja haittaohjelmien alkuperää kuvataan lehtijutuissa siis ristiriitaisesti, ja useista jutuista tulee lisäksi vaikutelma, että kilpajuoksu kyberturvallisuudesta vastaavien organisaatioiden ja kyberrikollisten välillä saa yhä mielikuvituksellisempia piirteitä.

Teksteissä hämäräksi jäävä inhimillinen toimijuus kertoo myös siitä, että kyberturvallisuuden diskursseissa ei ole yksioikoisia ”sankareita” tai ”vihollisia”. Taitava tietoverkkotoimija voi olla yhtä lailla hyvä tai paha hakkeri, tai jopa molempia yhtä aikaa (ks. Coleman 2014; Kubitschko 2015; Lehto ym. 2017, 19–20). Jos jonkinlaisia sankaruuden aineksia on kyberuhkista uutisoitaessa mahdollista löytää, tiedotusvälineet tarttuvat niihin hanakasti ja nostavat ne tekstien keskiöön. Kun paljastui, että yksittäinen kyberturvallisuuden tutkija oli onnistunut pysäyttämään WannaCry:n leviämisen, huomio kiinnittyi nopeasti hänen esimerkilliseen toimintaansa. Nimimerkillä MalwareTech (@malwaretechblog) julkisuudessa esiintynyt asiantuntija löysi haittaohjelman koodista niin sanotun tappokytkimen (*kill switch*), jonka avulla sen leviämistä saatiin merkittävästi hidastettua (Khomami & Solon 2017).

Siinä missä WannaCry kohdentui yksittäisiin käyttäjiin ja tietokoneisiin ja pyrki nopean leviämisensä kautta vähitellen halvaannuttamaan yritysten sisäisiä tietoverkkoja ja siten kokonaisia tietojärjestelmiä, organisaatiotason verkko-ongelmissa on usein toisenlainen logiikka. Esimerkiksi lokakuussa 2016 yhdysvaltalaiset käyttäjät huomasivat, että kirjautuminen suosituille sivustoille, kuten Netflixiin, Twitteriin ja Spotifyhin, ei onnistunut. Kyse oli massiivisesta kyberhyökkäyksestä, jonka tarkoituksena oli estää näiden sivustojen toiminta ja aiheuttaa yrityksille taloudellisia tappioita (BBC 2016; Menn, Finkle & Volz 2016). Tavallinen verkon käyttäjä ei voinut tehdä ongelmalle mitään, koska hyökkäys kohdistui sellaisiin internetin perustoimintoihin, joita ymmärtävät ja joihin pääsevät käsiksi vain alan ammattilaiset (Turunen 2016). Vaikka tämänkertainen DoS- eli palvelunestohyökkäys oli lyhytikäinen, se toimi ikävänä muistutuksena laajojen kuluttajapalveluiden haavoittuvuudesta, jossa yksittäisten käyttäjien tietoturvatoimilla ei ollut vaikutusta suuntaan tai toiseen.

Sekä syksyn 2016 että kevään 2017 suurten hyökkäysten yhteydessä tiedotusvälineet uutisoivat näyttävästi, että isojen kansainvälisten yritysten kyberturvallisuudessa on vakavia puutteita. Lokakuun hyökkäyksessä vuonna 2016 internetsivut hidastuivat, koska jopa 10 miljoonaan yksittäiseen koneeseen tunkeuduttiin ja ne liitettiin osaksi laajenevaa palvelunestoa (York 2016). Koska yksittäiset käyttäjät tai yritykset eivät

itse pystyneet torjumaan tunkeutumista, tilanteen selvittäminen jäi valtionhallinnon tehtäväksi (Edwards, Beech & Walsh 2016). Kyberiskujen vahingollisuuden ja yritysten varautumattomuuden korostaminen nosti uutisissa esiin valtion roolin. Kuten olemme tässä artikkelissa osoittaneet, valtio on kybermaailman keskeinen toimija: ainoastaan sillä on resursseja selvittää, kuinka tällaiset hyökkäykset torjutaan ja parhaimmassa tapauksessa ehkäistään ennalta.

Tietoverkkorikollisuuteen keskittyvä uutisointi sekä sen keskittyminen kyberhyökkäysten mittakaavaan ja hallitsemattomaan leviämiseen palveleekin valtion strategisia tavoitteita. Haittaohjelmat ja palvelunestohyökkäykset tuovat kyberuhkat osaksi internetin käyttäjien arkipäivää (tai ainakin muistuttavat niiden olemassaolosta), kun taas niistä uutisointi ei useinkaan paneudu iskujen taustalla oleviin rakenteisiin tai tekijöiden motiiveihin. Näin kyberrikollisuus säilyy julkisessa keskustelussa salaperäisenä mutta tuhopotentiaaliltaan huomattavana uhkana, joka assosioituu jopa informaatiovaikuttamiseen ja kybersotaan. Kun "uhan diskurssia" ylläpidetään, valtio voi tuottamissaan kyberstrategioissa helposti perustella, miksi sitä torjumaan tarvitaan puolustusvoimien erikoisyksiköitä ja osallistumista ylikansallisten yhteistyöelinten toimintaan. Kun vaikkapa EU:n lainvalvontaviraston Europolin uutisoidaan osallistuvan vuosittain ainakin 200 maailmanlaajuiseen kyberrikollisuuden vastaiseen operaatioon (Kippo 2017), lukija tulee muistutetuksi siitä, että kyberuhkia on kaikkialla, ne ovat vakavia, ja niiden torjuntaan täytyy tulevaisuudessa panostaa entistä enemmän.

Yksittäisiin käyttäjiin, yrityksiin ja tietojärjestelmiin kohdistuvien kyberiskujen ohella julkiseen keskusteluun on viime vuosina noussut runsaasti epäilyjä myös toisenlaisista kyberuhkista – poliittisesti motivoiduista, valtiollisen tason hyökkäyksistä – joiden toteutumiseen tiedotusvälineitä osallistetaan tavalla tai toisella (vrt. Jantunen 2015, 70–104). Tällainen kyberuhka tuntuu aktualisoituvan nykyisessä mediailmastossa erityisesti suurten yhteiskunnallisten tapahtumien kuten sotatilanteiden ja vaalien yhteydessä. Tällöin puhutaan usein informaatiovaikuttamisesta tai jopa -sodasta, jotka voidaan ymmärtää kybersodan rinnakkais- tai alakäsitteiksi. Informaatiosodankäynti on strategista viestintää, jonka avulla valtio pyrkii vaikuttamaan eri yleisöihin niihin kuhunkin vetoavien retoristen ja muiden viestintäkeinojen avulla. Informaatiooperaatioiden kohteena voivat olla niin oman maan kansalaiset kuin ulkovaltojenkin edustajat, ja keskeistä roolia niiden toteutuksessa näyttelevät perinteinen ja sosiaalinen media.

Esimerkiksi loppuvuodesta 2016 pidetyt Yhdysvaltain presidentinvaalit aiheuttivat useita kohuja. Ennen vaaleja vuodettiin demokraattiehdokas Hillary Clintonin sähköposteja, ja vaalien jälkeen Yhdysvaltain tiedustelupalvelu ilmoitti, että Venäjä on saattanut vaikuttaa vaalien lopputulokseen Donald Trumpin hyväksi (esim. Kähkönen 2016; Liimatainen 2016). Helmikuussa 2017 uutisoitiin Yhdysvaltain presidentin kansallisen turvallisuuden neuvonantajan Michael Flynnin erosta, joka johtui muun muassa liian läheisestä yhteydenpidosta Venäjän suurlähettiläässeen (Liimatainen & Eloranta 2017). Toukokuussa uutispommiksi nousi FBI:n pääjohtajan James Comeyn erottaminen, joka useiden lähteiden mukaan liittyy todellisuudessa Trumpin vaalivoiton Venäjä-sidosten tutkintaan (esim. Shear & Apuzzo 2017; Barrett, Entous & Rucker 2017).

Informaatiosodasta ja valtiollisista vaikuttamispyrkimyksistä kansallisen tason politiikkaan löytyy huomattavan monia muitakin esimerkkejä uutisteksteistä vuosilta 2016–2017. Erityisesti poliitikot ovat viime vuosina kärsineet tietomurroista, joissa on hyökätty heitä vastaan henkilöinä. Esimerkiksi toukokuussa 2017 internetiin vuoti Ranskan presidentinvaaliehdokkaan Emmanuel Macronin yksityisiä kampanjasähköposteja ja -asiakirjoja, joita oli muutettu hämmennyksen ja epäluulon aiheuttamiseksi (Skara & Burtsov 2017). Iskun tavoitteena oli vaikuttaa vaalien lopputulokseen vastaehdokkaan hyväksi. Kyse ei ollut ensisijaisesti siitä, että ehdokkaana oli Macron, vaan tietomurron taustalla vaikutti laajempi poliittinen konteksti: lehtitietojen mukaan hyökkääjät halusivat valtiojohtoon henkilön, joka sopi paremmin heidän omaan politiikkaansa.

Medialla on keskeinen merkitys siinä, miten informaatiovaikuttaminen etenee, mutta koska strategisen viestinnän taktinen taso toimii niin ennakoimattomasti, edes vakiintuneet tiedotusvälineet eivät yksin voi kontrolloida viestinnän leviämistä ja tulkintaa. Esimerkiksi Hillary Clintonin tapauksessa häntä itseään syytettiin aluksi välinpitämättömyydestä tietoturva-asioissa, mutta kun Venäjän osallisuus tapahtumiin varmistui, Clinton ikään kuin armahdettiin sekä median että kansalaisten silmissä. Toisaalta näyttää ilmeiseltä, että hänen maineensa oli kärsinyt jo häneen kohdistuvista epäilyistäkin. Tämä kertoo siitä, että informaatiovaikuttaminen on niin hienovaraista, että mediankin on vaikea tutkia asioiden todenperäisyys läpikotaisin. Vaikka uutisoinnin lähtökohtana olisikin pelkkä tapahtumien raportointi, todellisuudessa vaillinaiset tiedot voivat vain lisätä paniikkia ja pelkoa – mitä informaatiovaikuttamisella tietysti osaltaan tavoitellaankin.

Informaatiovaikuttaminen voi olla paljon muutakin kuin pelkästään poliitikoihin kohdistuvia kyberhyökkäyksiä. Kyberaikakauden varhaisimpina tiedon manipuloinnin muotoina voidaan pitää niin sanottuja nigerialaiskirjeitä, joiden tarkoituksena on huijata rahaa sähköpostitse tai sosiaalisessa mediassa valheellisten tarinoiden avulla (Halminen 2014). Toinen varhainen esimerkki informaatiovaikuttamisesta on joukkotiedotusvälineiden lähetysten ja satelliittiverkon häiritseminen (Sharma & Gupta 2002, 416). Nykyään tunnetuimpia informaatiovaikuttajia ovat Venäjän ja Kiinan valtiolliset propagandakoneistot, jotka tuottavat ristiriitaista informaatiota ja sytykkeitä itselleen myötämieliselle keskustelulle sekä maan sisällä että ulkomaisissa mediavälineissä (Jantunen 2010; Jantunen 2015; Nimmo 2015). Informaatiosota ja -vaikuttaminen käsitteinä kattavat siis hyvin monenlaisia toimintoja, joiden tulkinta riippuu siitä, missä kontekstissa ja tarkoituksessa niitä tarkastellaan.

Lopuksi

Kuten totesimme artikkelimme alussa, kyberturvallisuus ei liity ainoastaan teknologiaan, vaan sitä käsittelevien puheenvuorojen tulisi toimia osana yhteiskunnallisesti ja poliittisesti valveutunutta keskustelua maailman tilasta ja valtioiden välisistä suhteista. Olemme tässä artikkelissa tarkastelleet kybertoimintaympäristöön kytkeyty-

viä käsitteitä ja niiden historiaa, internetiä ja laajempaa tietoverkkoinfrastruktuuria, ”kyberiin” liitettyjä uhkia ja niiden moniulotteisuutta sekä esimerkinomaisesti kyberturvallisuuden artikuloitumista niin valtiollisissa strategioissa kuin tiedotusvälineiden julkaisemissa uutisissakin. Median osuus tässä tutkimuksessa on ollut toimia kontekstina, jossa kyberrikoksista hanakasti kirjoitetaan ja joka jopa huomaamattaan saattaa osallistua informaatiosodankäynnin operaatioihin. Olemme tällä yleisen tason tarkastelulla pyrkineet luomaan ”isoa kuvaa” ja ymmärrystä kyberturvallisuudesta yhteiskunnallisena ilmiönä. Keskeinen teema tässä tarkastelussa on ollut myös sen selvittäminen, millaisia rooleja eri toimijoille kybertoimintaympäristössä asemoituu.

Kybertoimintaympäristön perusperiaatteiden ymmärtäminen on tätä artikkelia kirjoitettaessa koettu tärkeäksi, sillä tähän kontekstiin liittyvät tutkimusperinteet ovat Suomessa vasta kehkeytymässä. Tietoverkkojen historia ja niille visioidut tulevaisuudet ovat tässä yhteydessä olennaisia. Maailmanlaajuisesti tarkasteltuna internetin suosio kasvaa edelleen: vuonna 2016 käyttäjiä oli maailmassa lähes 3,5 miljardia (Statista 2017). Jo varhaisen internetin kehitystyö perustui luottamukseen ja yhteisen edun tavoitteluun, ei vain teknologiaan. Kehittäjäyhteisö luotti siihen, että käyttäjät olivat ”enemmän tai vähemmän kykeneviä ja sydämiltään riittävän puhtaita, etteivät he tarkoituksella tai huolimattomuuttaan häiritse verkkoa” (Zittrain 2008, 3). Sittemmin verkosta on tullut suljetumpi. Internetin alkujaan generatiivinen luonne, eli vapaa muokattavuus, on lopulta kääntynyt itseään vastaan. Internet kärsii nykyään jatkuvista virusepidemioista ja haittaohjelmista, ja myös uusia uhkia ilmaantuu näköpiiriin. On luultavaa, että yhä useampi internetin käyttäjä kaipaa verkkoon lisää kontrollia ja stabiiliutta (vrt. Zittrainin 2008, 3), ja sitä, että edes ymmärrettäisiin, ketä tai mitä vastaan kyberturvallisuudessa on tarpeen suojautua.

Rikollisuus, vakoilu ja sota ovat merkittävimpiä kybermaailman uhkia. Niiltä suojautuakseen yksittäinen ihminen ei voi juuri muuta kuin muuttaa omaa käytöstään kybertoimintaympäristössä: varmistamalla sähköpostien olevan oikealta lähettäjältä, vaihtamalla salasanansa riittävän usein ja pitämällä huolta tietoturvastaan. Valtiovallan tehtävä on pysäyttää tai saattaa kuriin rikollinen toiminta. Tehtävä ei kuitenkaan ole yksinkertainen, sillä länsimaisissa demokratioissa ei mukisematta hyväksytä valtiovallan puuttumista kansalaisen yksityiseen verkkokäyttäytymiseen. Toisaalta myös valtiot voivat itsessään olla kansalaisilleen yhtä iso uhka kuin kuka tahansa muu kybermaailman toimija. Rikollista toimintaa voivat harjoittaa myös valtioiden tukemat yritykset, minkä lisäksi on yleisesti tiedossa, että maailmanpoliittisesti merkittävien maiden tiedustelupalvelut tarkkailevat yksityishenkilöitä heidän tietämättään. (Kubitschko 2015.)

Kyberturvallisuusstrategiat ovat keino hälventää ristiriitaista käsitystä valtioista kansalaisten valvojina ja vakuuttaa heidät siitä, että valtion toimet kybermaailmassa ovat heidän parhaakseen. Strategiat voivat herättää kansallista yhtenäisyyden tunnetta ja ylpeyttä oman maan saavutuksista, eikä niihin sisäänkirjoitettua ideologiaa ole vaikea liittää osaksi omaa ajattelua. (Jansson 2017, 90.) On todennäköistä, ettei yksittäinen internetin käyttäjä koe kybermaailman ongelmia niin ratkaisevina kuin miten ne kyberturvallisuusstrategioissa kuvataan. Tulevaisuudessa ongelmia voi kui-

tenkin syntyä, vaikkei julkinen kyberkeskustelu juuri nyt vaikuttaisikaan kovin kiinnostavalta.

Valtioiden kyberturvallisuusstrategiat ovat yleisesti kenen tahansa saatavilla, joten jos valtio päättää toteuttaa strategioissaan esittämiään muutoksia ja kansalaiset osoittavat eriävän mielipiteen, valtio voi aina vedota strategian julkisuuteen. Esimerkiksi lakimuutokset, jotka mahdollistavat laajamittaisemman tiedustelun tai tietoturvaohjelman asentaminen pakolliseksi internetiä käyttäviin laitteisiin, ovat herättäneet keskustelua yksityisyydensuojasta ja sananvapaudesta. Vuosina 2017–2018 Suomessa on neuvoteltu tiedustelulainsäädännön kiireellisestä uudistamisesta, joka toteutuessaan mahdollistaisi entistä tiiviimmän kansalaisten valvonnan (Halminen & Kempas 2017). Kyberturvallisuusstrategioiden pyrkimysten ja kyberturvallisuuteen liittyvien keskustelujen ymmärtäminen on tärkeää myös tavallisen kansalaisen näkökulmasta.

Saara Jantunen (2010, 41) huomauttaa, että vaikka terrorismi ja kyberuhka voivat käytännössä tarkoittaa hyvin samanlaisia operaatioita, niiden herättämät assosiaatiot ovat aivan erilaisia: siinä missä terrorismi edustaa pahuutta, taantumusta ja vierauden pelkoa, "kyber" viittaa korkean tason teknologiaan ja länsimaiseen edistykseen. Kyberdiskurssissa monet sodankäynnin ja kansainvälisen politiikan lainalaisuudet monimutkaistuvat ja kääntyvät jopa päälaelleen. Kyberuhkat eivät välttämättä tule valtion rajojen ulkopuolelta, ja myös valtio itse voi osallistua kyberrikollisuuteen, ainakin epäsuorasti. Informaatiosodankäynnissä valtio saattaa viestittää omille kansalaisilleen yhtä ja vieraan vallan edustajille toista, mutta kuten olemme tässä artikkelissa osoittaneet, rikoksen, epäeettisen toiminnan ja uhkien torjumisen väliset rajat ovat kybertoimintaympäristön monimuotoisuudesta johtuen häilyviä. Lisäksi aihetta koskeva lainsäädäntöprosessi on kesken ja teknologinen kehitys muuttaa sekä ymmärrystä kyberturvallisuudesta että siitä käytävän keskustelun käsitteistöä.

Median tehtävänä on varmistaa tiedonvälitys kybertoimintaympäristön tapahtumista sekä tapahtumien tulkinta ja kontekstointi tavalliselle internetin käyttäjälle. Tahtomattaan se on kuitenkin samalla mukana myös valtiotoimijoiden keskinäisessä kamppailussa välittäessään tietoa suurelle yleisölle ja tarjotessaan julkisia keskusteluforumeita. Yhtäältä on tärkeää julkaista poliittisesti keskeisiä uutisia objektiivisesti, mutta toisaalta median vastuulla on myös julkishallinnon valvonta ja kritiikki. Jos valtionhallinto ei pysty antamaan tai halua antaa medialle riittävästi olennaista ja uutiskynnyksen ylittävää tietoa, mediasta voi jopa tulla yksi informaatiosodan osapuolista. Näin kävi Suomessa esimerkiksi joulukuussa 2017, kun *Helsingin Sanomat* julkaisi omaaloitteisesti salaisia hallinnon asiakirjoja varmistaakseen omien sanojensa mukaan kansalaisten edun tiedustelulainsäädännön uudistuksessa (Halminen & Pietiläinen 2017c). Kuten tämä esimerkki kuvastaa, ja kuten olemme tässä artikkelissa perustelleet, toimivat tietoliikenne- ja viestintäjärjestelmät ovat keskeinen osa yhteiskunnan perusinfrastruktuuria. Niiden kytkeytyminen erilaisten poliittisten etujen ajamiseen ja jopa kansainvälisen tason informaatiovaikuttamiseen on monimutkainen kokonaisuus, johon liittyvää kriittistä tutkimusta tarvitaan kipeästi lisää.

Media-aineisto

Barrett, Devlin; Entous, Adam & Rucker, Philip (2017). President Trump fires FBI Director Comey. *Washington Post* 10.5.2017. https://www.washingtonpost.com/world/national-security/comey-misstated-key-clinton-email-evidence-at-hearing-say-people-close-to-investigation/2017/05/09/074c1c7e-34bd-11e7-b373-418f6849a004_story.html

BBC (2014). Sony PlayStation Network and other game services attacked. BBC 25.8.2014. http://www.bbc.com/news/technology-28925052

BBC (2016). Cyber attacks briefly knock out top sites. BBC 21.10.2016. http://www.bbc.com/news/technology-37728015

BBC (2017). Massive ransomware infection hits computers in 99 countries. BBC 13.5.2017. http://www.bbc.com/news/technology-39901382

Edwards, Julia; Beech, Eric & Walsh, Eric (2016). FBI investigating cause of cyber attacks: law enforcement official. *Reuters* 21.10.2016. http://www.reuters.com/article/us-usa-cyber-fbi-idUSKCN12L2P2

Gellman, Barton; Blake, Aaron & Miller, Greg (2013). Edward Snowden comes forward as source of NSA leaks. *Washington Post* 9.6.2013. https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html

Halminen, Laura (2014). Liian helppoa rahaa ollakseen totta – näin toimii nigerialaiskirje ja neljä muuta huijausta. *Helsingin Sanomat* 26.10.2014. http://www.hs.fi/kotimaa/art-2000002772494.html

Halminen, Laura & Kempas, Karla (2017). Tiedustelulain luonnoksessa on asiantuntijoiden mukaan korjattavaa – ”Vaikka kuinka monta kertaa hoetaan, ettei kyse ole massavalvonnasta, niin sitä se on”. *Helsingin sanomat* 19.4.2017. http://www.hs.fi/politiikka/art-2000005177146.html

Halminen, Laura & Pietiläinen, Tuomo (2017a). Lakiluonnos toisi Supolle ja Puolustusvoimille uusia laajoja keinoja tiedusteluun – HS perkasi ehdotusten sisällön. *Helsingin Sanomat* 19.4.2017. http://www.hs.fi/politiikka/art-2000005176089.html

Halminen, Laura & Pietiläinen, Tuomo (2017b). ”Pakettien sieppaamista” ja käsin avaamista: Tätä tietoliikennetiedustelu tarkoittaisi. *Helsingin Sanomat* 19.4.2017. http://www.hs.fi/politiikka/art-2000005176117.html

Halminen, Laura & Pietiläinen, Tuomo (2017c). Salaisuus kallion uumenissa – juuri kukaan ei tiedä, mitä tekee Puolustusvoimien Viestikoekeskus, mutta nyt HS:n saamat asiakirjat avaavat mysteerin. *Helsingin Sanomat* 16.12.2017. https://www.hs.fi/politiikka/art-2000005492284.html

Happonen, Päivi (2017). Analyysi: Päätyvätkö salaiset rakkausviestimme Supon tiedusteluhaaviin? Yle Uutiset 19.4.2017. https://yle.fi/uutiset/3-9571907

Jokiniemi, Emmakaisa (2017). Miten yli 150 maahan levinnyt verkkohyökkäys paisui niin isoksi? Asiantuntija: Hyökkäyksen tekninen taso kuin vuoden 2003 verkkomadoissa. Yle Uutiset 15.5.2017. https://yle.fi/uutiset/3-9612993

Kauhanen, Anna-Liina (2015). Työryhmä ehdottaa armeijalle ja poliisille lupaa verkkotiedusteluun – viestintäministeriö vastustaa kiivaasti. *Helsingin Sanomat* 11.1.2015. http://www.hs.fi/kotimaa/art-2000002791447.html

Khomami, Nadia & Solon, Olivia (2017). “Accidental hero” halts ransomware attack and warns: this is not over. *The Guardian* 13.5.2017. https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack

Kippo, Johanna (2017.) Hurja kyberhyökkäys jatkuu – iskenyt jo 150 maahan ja 200 000 kohteeseen. *Yle Uutiset* 14.5.2017. https://yle.fi/uutiset/3-9612491

Kokkonen, Yrjö (2017). Tuhoisa haittaohjelma sulkee tietokoneita kymmenissä maissa – kehitetty USA:n turvallisuusvirastossa? *Yle Uutiset* 13.5.2017. https://yle.fi/uutiset/3-9611520

Koutonin, Mawuna (2017). No business, no boozing, no casual sex: when Togo turned off the internet. *The Guardian* 21.9.2017. https://www.theguardian.com/global-development/2017/sep/21/no-business-no-boozing-no-casual-sex-when-togo-turned-off-the-internet

Incoronato, Katja (2017). Tästä tiedustelulaissa on kyse – Kansanedustaja: ”On tosiasiassa estetty useita terrori-iskuja”. *Uusi Suomi* 20.8.2017. https://www.uusisuomi.fi/kotimaa/227970-tasta-tiedustelulaissa-kyse-kansanedustaja-tosiasiassa-estetty-useita-terrori-iskuja

Kähkönen, Virve (2016). Hillary Clintonin annettava kirjallinen todistus sähköpostiskandaalissa – kohu varjostaa vaalikampanjaa. *Helsingin Sanomat* 20.8.2016. http://www.hs.fi/ulkomaat/art-2000002916961.html

Leipola, Lasse (2017). Onko urkinnalla oikeasti niin kova kiire? *Vihreä Lanka* 20.4.207. http://www.vihrealanka.fi/uutiset-kotimaa/onko-urkinnalla-oikeasti-niin-kova-kiire

Liimatainen, Karoliina (2016). CIA: Venäjä pyrki auttamaan Trumpia presidentin vaaleissa. *Helsingin Sanomat* 10.12.2016. http://www.hs.fi/ulkomaat/art-2000005001541.html

Liimatainen, Karoliina & Eloranta, Ville (2017). Trumpin neuvonantaja Michael Flynn on eronnut tehtävästään – väitteet Venäjän-yhteyksistä olivat lopulta liikaa. *Helsingin Sanomat* 14.2.2017. http://www.hs.fi/ulkomaat/art-2000005087004.html

Mansikka, Ossi (2017). Hakkeriyhteisö sanoo löytäneensä puutteita autoihin asennettavan "mustan laatikon" tietoturvasta – Trafi testannut vastaavia laitteita. *Helsingin Sanomat* 16.1.2017. http://www.hs.fi/kotimaa/art-2000005046813.html.

Menn, Joseph; Finkle, Jim & Volz, Dustin (2016). Cyber attacks disrupt PayPal, Twitter, other sites. *Reuters* 21.10.2016. http://www.reuters.com/article/us-usa-cyber-idUSKCN12L1ME

Miikkulainen, Lauri (2017). Kyberturvallisuuden asiantuntija: Turun puukotukset ovat viimeinen herättäjä uuden tiedustelulain tarpeellisuudelle. *Yle Uutiset* 23.8.2017. https://yle.fi/uutiset/3-9792529

Moore, Michael (2017). Google, Yahoo and PlayStation PSN – 13 of the biggest cyber-attacks of ALL TIME. Sunday Express, express.co.uk 12.2.2017. http://www.express.co.uk/life-style/science-technology/765848/Google-Yahoo-PSN-biggest-cyber-attacks-hacks-viruses-data-breaches-ever

Mäntymaa, Eero (2017). Olisiko tiedustelulaki estänyt Turun iskun? Tuskin, sanovat lakiasiantuntijat. Yle Uutiset 23.8.2017. https://yle.fi/uutiset/3-9791280

Naughton, John (2016a). Britain's cybersecurity policy needs common sense, not just cash. *The Guardian* 6.11.2016. https://www.theguardian.com/commentisfree/2016/nov/06/uk-cybersecurity-needs-common-sense-not-just-cash.

Nimmo, Ben (2015). Anatomy of an info-war: How Russia's propaganda machine works, and how to counter it. https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/

Phillips, Tom (2016). Five years ago today, Sony admitted the great PSN hack. *Eurogamer* 26.4.2016. http://www.eurogamer.net/articles/2016-04-26-sony-admitted-the-great-psn-hack-five-years-ago-today

Postila, Tapani (2017). Kaukopartio kyberin korvessa. Pääkirjoitus 22.2.2017, *Keskipohjanmaa*. https://www.keskipohjanmaa.fi/131750/kaukopartio-kyberin-korvessa/s/fb1ea1a6

Rydman, Arno (2017). Suomi on 10 vuotta muita perässä tiedustelussa – ja maailma on muuttunut. *Verkkouutiset* 12.7.2017. https://www.verkkouutiset.fi/kotimaa/Tiedustelulaki-67780

Shear, Michael D. & Apuzzo, Matt (2017). F.B.I. Director James Comey Is Fired by Trump. *The New York Times* 9.5.2017. https://www.nytimes.com/2017/05/09/us/politics/james-comey-fired-fbi.html

Skara, Marija & Burtsov, Petri (2017). Satoja Macronin kampanjan asiakirjoja vuodettiin julkisuuteen. *Yle Uutiset* 6.5.2017. http://yle.fi/uutiset/3-9598568

Solon, Olivia (2016). Hacking group auctions 'cyber weapons' stolen from NSA. *The Guardian* 16.8.2016. https://www.theguardian.com/technology/2016/aug/16/shadow-brokers-hack-auction-nsa-malware-equation-group

Thielman, Sam (2016). Yahoo hack: 1bn accounts compromised by biggest data breach in history. *The Guardian* 15.12.2016. https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached

Tolkki, Kristiina (2017). Suojelupoliisi saamassa oikeudet verkkotiedusteluun: Suomi haluaa suojautua terrorismilta ja vakoilulta. *Yle Uutiset* 19.4.2017. https://yle.fi/uutiset/3-9570943

Turunen, Petri (2016). Oletko havainnut hitautta netissä? Meneillään on suuri verkkohyökkäys. *Ilta-Sanomat* 21.10.2016. http://www.iltasanomat.fi/digitoday/art-2000001935958.html

York, Kyle (2016). Dyn Statement on 10/21/2016 DDoS Attack. Dyn 22.10.2016. https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

Strategia-asiakirjat

CCDCOE (2016). *Cyber Security Strategy Documents*. https://ccdcoe.org/cyber-security-strategy-documents.html

ENISA (2014). *An Evaluation Framework for National Cyber Security Strategies*. ENISA, Heraklion. https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies

Lehto, Martti; Limnéll, Jarno; Innola, Eeva; Pöyhönen, Jouni; Rusi, Tarja & Salminen, Mirva (2017). *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi*. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017. Helsinki: Valtioneuvoston kanslia. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160233/Suomen_kyberturvallisuuden_nykytila,__tavoitetila_ja.pdf

OECD (2012). Cybersecurity Policy Making at a Turning Point. Analysing a new generation of national cybersecurity strategies for the Internet economy. *OECD Digital Economy Papers*, No. 211, OECD Publishing. https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Puolustusministeriö (2013). *Suomen kyberturvallisuusstrategia*. Valtioneuvoston periaatepäätös 24.1.2013. https://www.turvallisuuskomitea.fi/index.php/fi/mcdc/14-suomen-kyberturvallisuusstrategia

Puolustusministeriö (2017a). *Yhteiskunnan turvallisuusstrategia*. Valtioneuvoston periaatepäätös 2.11.2017. https://www.turvallisuuskomitea.fi/index.php/files/35/YTS2017%20materiaalit/80/YTS_2017_suomi.pdf

Puolustusministeriö (2017b). *Valtioneuvoston puolustusselonteko*. Valtioneuvoston kanslian julkaisusarja 5. https://defmin.fi/files/3683/J05_2017_VN_puolustusselonteko_Su_PLM.pdf

Sisäministeriö (2017a). *Siviilitiedustelulainsäädännön valmistelu*. http://intermin.fi/tiedustelu

Sisäministeriö (2017b). *Siviilitiedustelulainsäädäntö. Siviilitiedustelulakityöryhmän mietintö*. Sisäministeriön julkaisu 8. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79759/SM_08_2017_Siviilitiedostelulainsaadanto.pdf

The White House (2008). *National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23).* 8.1.2008. https://fas.org/irp/offdocs/nspd/nspd-54.pdf

Tikk, Eneken; Kaska, Kadri; Rünnimeri, Kristel; Kert, Mari; Talihärm, Anna-Maria & Vihul, Liis (2008). Cyber Attacks Against Georgia: Legal Lessons Identified. *NATO Unclassified Version 1.0*. http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf

Valtioneuvoston kanslia (2004). *Suomen turvallisuus- ja puolustuspolitiikka 2004*. Valtioneuvoston kanslian julkaisusarja 16. http://www.defmin.fi/files/240/2493_2161_Selonteko_2004_1_.pdf

Kirjallisuus

872/2011 (2011) Poliisilaki. http://www.finlex.fi/fi/laki/alkup/2011/20110872

1467/2011 (2011) Laki pakkokeinolain 5 a luvun 2 ja 4 §:n muuttamisesta. http://www.finlex.fi/fi/laki/alkup/2011/20111467

Candolin, Catharina (2012). Saako sanoa kyber? *All Things Cyber* -blogi. http://kyberturvallisuus.blogspot.fi/2012/03/saako-sanoa-kyber.html

Choucri, Nazli; Madnick, Stuart & Ferwerda, Jeremy (2014). Institutions for cyber security: international responses and global imperatives. *Information Technology for Development* 20: 2, 96–121.

Coleman, Gabrielle (2014). *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London: Verso.

Curran, James (2012). Rethinking Internet history. Teoksessa: James Curran, Natalie Fenton & Des Freedman (toim.). *Misunderstanding the Internet*. Lontoo & New York: Routledge. 34–65.

van Dijck, José (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society* 12(2), 197–208.

e-Estonia (2017). Estonian e-Residency. https://e-estonia.com/e-residents/about/

Eduskunta (2017). *Eduskunnan täysistunnot, Helsinki-Korp-versio* [tekstikorpus]. Kielipankki. http://urn.fi/urn:nbn:fi:lb-2017020202

Gamreklidze, Ellada (2014). Cyber security in developing countries, a digital divide issue. *The Journal of International Communication* 20: 2, 200–217.

Hamilton, Sheryl N. (1998). Incomplete determinism: A discourse analysis of cybernetic futurology in early cyberculture. *Journal of Communication Inquiry* 22:2, 177–204.

Jansson, Saara (2017). *Kansallisten kyberstrategioiden diskurssit*. Julkaisematon viestintätieteiden pro gradu -tutkielma. Vaasan yliopisto.

Jantunen, Saara (2010). *Uusien uhkakuvien luominen: tapaus 'kiinalaiset kybersoturit'. Lingvistinen uhka-analyysi kyberdiskurssista*. Maanpuolustuskorkeakoulun Johtamisen ja sotilaspedagogiikan laitoksen Julkaisusarja 1, tutkimuksia 4. Helsinki: Maanpuolustuskorkeakoulu. http://www.doria.fi/bitstream/handle/10024/74116/jantunen-uusien_uhkakuvien_luominen.pdf

Jantunen, Saara (2015). *Infosota*. Helsinki: Otava.

Johnson, Mark (2013). *Cyber Crime, Security and Digital Intelligence.* Lontoo & New York: Routledge.

Kansalliskirjasto (2011). *Kansalliskirjaston sanoma- ja aikakauslehtikokoelman suomenkielinen osakorpus, Kielipankki-versio* [tekstikorpus]. Kielipankki. http://urn.fi/urn:nbn:fi:lb-2016050302

Kubitschko, Sebastian (2015). The role of hackers in countering surveillance and promoting democracy. *Media and Communication*, 3(2), 77–87. http://dx.doi.org/10.17645/mac.v3i2.281

Lawson, Sean (2012). Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States. *First Monday*, 17(7). http://dx.doi.org/10.5210/fm.v17i7.3848

Limnéll, Jarno (2014). *Kyber rantautui Suomeen.* Aalto yliopiston julkaisusarja Tiede + Teknologia 12. Helsinki: Aalto yliopisto.

Limnéll, Jarno; Majewski, Klaus & Salminen, Mirva (2014). *Kyberturvallisuus*. Saarijärvi: Docendo.

Lin, Herbert S. (2010). Offensive cyber operations and the use of force. *Journal of National Security Law & Policy* 4: 63, 63–86.

Luiijf, Eric; Besseling, Kim & de Graaf, Patrick (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures* 9: 1, 3–31.

Luiijf, Eric; Besseling, Kim; Spoelstra, Maartje & de Graaf, Patrick (2011). Ten national cyber security strategies: A Comparison. Teoksessa: Sandro Bologna, Dimitris Gritzalis, Bernhard Hämmerli & Stephen Wolthusen (toim.). *Critical Information Infrastructure Security: 6th International Workshop, CRITIS 2011, Lucerne, Switzerland, September 8-9, 2011, Revised Selected Papers.* Lontoo: Springer. 1–17.

McGraw, Gary (2013). Cyber war is inevitable (Unless we build security in). *Journal of Strategic Studies* 36: 1, 109–119.

Min, Kyoung-Sik; Chai, Seung-Woan & Han, Mijeong (2015). An international comparative study on cyber security strategy. *International Journal of Security and Its Applications* 9: 2, 13–20.

Mindell, David A (2003). *Between Human and Machine: Feedback, Control, and Computing before Cybernetics*. Baltimore: The Johns Hopkins University Press.

Naughton, John (2016b). The evolution of the Internet: from military experiment to General Purpose Technology. *Journal of Cyber Policy* 1: 1, 5–28. https://doi.org/10.1080/23738871.2016.1157619

Pelican, Luke (2012). Peacetime Cyber-espionage: A dangerous but necessary game. *CommLaw conspectus* 20: 2, 363–390.

Pälli, Pekka; Vaara, Eero & Sorsa, Virpi (2009). Strategy as text and discursive practice: a genre-based approach to strategizing in city administration. *Discourse & Communication* 3: 3, 303–318.

Richards, Julian (2014). *Cyber-War: The Anatomy of the Global Security Threat*. Hampshire & New York: Palgrave Macmillan.

Rudner, Martin (2013). Cyber-threats to critical national infrastructure: an intelligence challenge. *International Journal of Intelligence and Counter Intelligence* 26: 3, 453–481. https://doi.org/10.1080/08850607.2013.780552

Sabillon, Regner; Cavaller, Victor & Cano, Jeremy (2016). National cyber security strategies: global trends in cyberspace. *International Journal of Computer Science and Software Engineering* (IJCSSE) 5: 5, 67–81.

Saloharju, Aleksi (2015). *Kehitystä, epävarmuutta ja orastavaa alueellisuutta: Käsitykset kyberturvallisuudesta valtioiden kyberturvallisuusstrategioissa*. Julkaisematon yhteiskuntatieteiden pro gradu -tutkielma. Turun yliopisto.

Salter, Michael & Bryden, Chris (2009). I can see you: harassment and stalking on the Internet. *Information & Communications Technology Law* 18: 2, 99–122.

Sanastokeskus (2017) *Kokonaisturvallisuuden sanasto* (TSK 50). Sanastokeskus TSK: Helsinki. https://www.turvallisuuskomitea.fi/index.php/files/35/YTS2017%20materiaalit/78/Kokonaisturvallisuuden_sanasto.pdf

Schjolberg, Stein (2014). *The History of Cybercrime: 1976–2014*. Norderstedt: Cybercrime Research Institute GmbH.

Sessions, Jonathan (2014). The legal aspects of streaming digital media from the internet. Unpublished Master's Thesis. Utica College. http://search.proquest.com/openview/330392ee7107db4a2933b3a8315d269e/1.pdf

Shackelford, Scott & Craig, Amanda (2014). Beyond the new 'digital divide': analyzing the evolving role of national governments in internet governance and enhancing cybersecurity. Research Paper Number 290. 50 STAN. J. INT'L L. 119. Social Science Research Network electronic library. http://ssrn.com/abstract=2446666

Sharma, Sushil K. & Gupta, Jatinder N.D. (2002). Securing information infrastructure from information warfare. *Logistics Information Management* 15: 5/6, 414–422.

Singer, P. W. & Friedman, Allan (2014). *Cybersecurity and Cyberwar. What Everyone Needs to Know®*. New York: Oxford University Press.

von Solms, Rossouw & van Niekerk, Johan (2013). From information security to cybersecurity. *Computers & Security* vol. 3, 97–102.

Statista (2017). *Number of internet users worldwide from 2005 to 2016* (in millions). https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

Suomi.fi (2017) Sähköinen tunnistus ja allekirjoitus. https://www.suomi.fi/suomifi/suomi/asioi_verkossa/sahkoinen_tunnistus_ja_allekirjoitus/index.html

Thompson, Karson K. (2011). Not like an Egyptian: cybersecurity and the Internet kill switch debate. *Texas Law Review*, 90, 465.

Viljanen, Vesa (2017) Lainsäädäntö. *Yksityisyydensuoja.fi*. https://www.yksityisyydensuoja.fi/lains%C3%A4%C3%A4d%C3%A4nt%C3%B6

Warner, Michael (2012). Cybersecurity: A Pre-history. *Intelligence and National Security* 27(5): A Decade of Intelligence Beyond 9/11: Security, Diplomacy and Human Rights, 781–799. http://dx.doi.org/10.1080/02684527.2012.708530

Zittrain, Jonathan (2008). *The Future of the Internet – And How to Stop It*. New Haven & London: Yale University Press.