IV. Mirva Salminen (2021) Arkipäivän digitaalinen turvallisuus Euroopan pohjoisilla alueilla: tapaustutkimus Tunturi-Lapista. *Media ja viestintä* 44(1), 158–180. https://doi.org/10.23983/mv.107305.

Artikkeli

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

Arkipäivän digitaalinen turvallisuus Euroopan pohjoisilla alueilla

Tapaustutkimus Tunturi-Lapista

Digitalisaatio muuttaa yksilöiden ja yhteisöjen elämää Euroopan pohjoisilla alueilla merkittävästi, mutta millaisiksi ihmiset kokevat muutokset? Millaisia mahdollisuuksia, toiveita, haasteita ja huolia kehitykseen liittyy? Artikkelissa tarkastellaan digitalisaatiota ja kyberturvallisuutta laajasta inhimillisen turvallisuuden näkökulmasta. Tarkastelu perustuu Enontekiöllä marraskuussa 2018 pidettyihin työpajoihin, joissa keskusteltiin digitalisaation vaikutuksista arkipäivässä. Koska kyberturvallisuudessa suojattaviksi kohteiksi ovat vakiintumassa tieto ja yhteiskunnan kannalta kriittiseksi arvioitu infrastruktuuri tai toiminnot, artikkelissa käytetään digitaalisen turvallisuuden käsitettä. Suojaamisen kohteina ovat tällöin yksilöt ja yhteisöt digitalisoituvassa arkipäivässään. Ihmiset ovat myös keskeisiä digitaalisen turvallisuuden tuottajia, joiden tulisi osallistua tavoiteltavien arvojen, näihin kohdistuvien uhkien ja turvatoimien määrittelyyn sekä näitä koskevaan päätöksentekoon. Keskeinen johtopäätös työpajakeskusteluista on, että digitalisaatiota pitäisi ohjata suuntaan, jossa paikallisuus ja inhimilliset tarpeet ja rajoitteet tulevat paremmin huomioiduiksi.

AVAINSANAT: digitalisaatio, arkipäivän turvallisuus, digitaalinen turvallisuus, kyberturvallisuus, harvaan asutut alueet

Enontekiö on pinta-alaltaan Suomen kolmanneksi suurin mutta väestöltään vain noin 2 000 asukkaan kunta Tunturi-Lapissa. Poroja alueella elää yli 20 000. Kunta sijaitsee saamelaisten kotiseutualueella, Ruotsin ja Norjan rajalla. Siellä on noin 60 prosenttia Suomen tuntureista, laajat erämaa-alueet ja merkittäviä vesistöjä. Terminen talvi kestää yli puoli vuotta. Puolet vuotuisesta sademäärästä tulee lumena. Kunnan keskeisimmät elinkeinot ovat palvelutuotanto (noin 75 prosenttia, ml. julkispalvelut ja turismi), jalostus (noin 10 prosenttia) ja alkutuotanto (noin 10 prosenttia).[1] Maantietä pitkin etäisyys kuntakeskus Hetasta Rovaniemelle, ”Lapin pääkaupunkiin”, on noin 300 kilometriä. Suurin piirtein sama etäisyys on Norjan puolelle Tromssaan ja Ruotsin puolelle Kiirunaan. Etäisyyksien, maantieteellisten olosuhteiden ja väestön vähäisyyden vuoksi esimerkiksi suuri osa peruspalveluista on enontekiöläisille tuotettu jo pitkään digitalisaation mahdollistamin keinoin.

Tunturi-Lapissa[2] digitalisaatio etenee julkishallintovetoisesti. Laajoilla, vähäväkisillä alueilla yritykset eivät katso markkinaehtoista informaatioinfrastruktuurin rakentamista kannattavaksi. Enontekiöllä ei ole kattavaa valokuituverkkoa, mutta esimerkiksi Karesuvannolle on rakennettu kyläverkko Euroopan maaseuturahaston tuella[3]. Vuoden 2019 alussa suomalaisen ja norjalaisen yrityksen valokuituverkot yhdistettiin Kilpisjärven kautta, mikä lisäsi vika- ja häiriösietoisuutta alueella[4]. Kiinteän laajakaistan saatavuus Enontekiöllä oli vuoden 2019 lopussa Liikenne- ja viestintäviraston tilastojen mukaan 100 Mbit/s 11 prosentissa kotitalouksista, 30 Mbit/s 18 prosentissa kotitalouksista, 10 Mbit/s 38 prosentissa kotitalouksista ja 2 Mbit/s 54 prosentissa kotitalouksista[5]. Saman viraston alainen MONITORi-palvelu antaa samansuuntaisia tietoja kiinteästä laajakaistasta[6], mutta listaa myös mobiiliverkon kattavuuden. Enontekiöllä 89,8 prosenttia kotitalouksista on vähintään 30 Mbit/s 4G:n kattavuusalueella. Yleispalveluvelvoitteen[7] mukainen palveluntarjoaja löytyy Hetan alueelta ja osin Pöyrisjärven ja Puljun erämaa-alueilta.[8] Suurin osa Tunturi-Lapista on todennäköisesti jatkossakin mobiiliyhteyksien varassa[9].

Digitalisaation tunkeutuessa syvälle yhteiskunnan rakenteisiin on oleellista tarkastella niitä vaikutuksia, joita muutoksella on yksilöiden ja yhteisöjen kokemalle osallisuudelle, luottamukselle ja turvallisuudelle. Kokemukset eivät ole yhteneväiset koko maassa, vaan vaihtelevat alueellisesti. Enontekiö valikoitui tutkimustapaukseksi digitalisaatioon liittyvistä arkipäivän turvallisuustekijöistä Euroopan pohjoisilla alueilla[10], koska kunnassa yhdistyvät monet näiden alueiden erityispiirteet, kuten edellä mainitut pitkät etäisyydet, haastavat olosuhteet ja harva asutus sekä elinkeinojen rajallisuus, kunnan taloudelliset paineet ja luonnonkiertoon liittyvä elämäntapa. Tulevaisuudessa digitalisaatio muuttaa yksilöiden ja yhteisöjen arkipäivää yhä voimakkaammin, sillä sitä tarjotaan ja hyödynnetään ratkaisuna edellä mainittuihin haasteisiin[11]. Digi- ja väestötietoviraston digitalisaation edistämisen ohjelman mukaan vuoteen 2023 mennessä julkishallinnon palvelut on suurelta osin digitalisoitu: kansalaiset hoitavat asioinnin pääosin sähköisesti ja yritykset kokonaan[12]. Mutta mitkä asiat ihmiset kokevat nopeasti etenevässä digitalisaatiossa hyödyllisiksi ja mitkä haitallisiksi? Katsovatko Enontekiön asukkaat voivansa vaikuttaa kehityksen suuntaan? Millaisia toiveita ja haasteita digitalisaatioon ja sen arkipäivässä aiheuttamiin muutoksiin liittyy? Näitä kysymyksiä pohdittiin kahdessa marraskuussa 2018 järjestetyssä työpajassa. Tässä artikkelissa käyn teemoitellusti läpi työpajakeskusteluissa esiin nousseita digitaalisen turvallisuuden tekijöitä. Tavoitteena on laajan yleiskuvauksen koostaminen digitalisaation vaikutuksista Tunturi-Lapissa (ks. Guest, MacQueen ja Namey. 2012, 27–28, 30–31).

Digitaaliseen turvallisuuteen liittyviä eriarvoistavia ja arkipäivässä huolta aiheuttavia ulottuvuuksia on aiemmin tarkasteltu esimerkiksi digitaalisia kuiluja, (digitaalisten) ihmisoikeuksien toteutumista ja ihmisten osaamista ja oppimista koskevissa tutkimuksissa (esim. Junger, Montoya ja Overink 2017; Pare 2005; Wagner, Kettermann ja Veith 2019; Wheeler, 2013). Ihmisten käyttäytymistä ja kokemuksia digitaalisessa toimintaympäristössä ja tämän ympäristön rakenteen vaikutuksia vuorovaikutukseen on tutkittu esimerkiksi keskustelupalstojen ja sosiaalisen median osalta (van Dijck 2013; Saariketo 2015; Stiff 2019; Vainikka ja Harju 2019) sekä kaupallisen tiedonkeruun ja yksityisyyden suhteeseen liittyen (van Dijck 2013; Montgomery 2015; Sirkkunen 2016). Tutkimusta digitalisaation vaikutuksista ihmisten ja yhteisöjen arkipäivään Euroopan pohjoisilla alueilla on tehty suhteellisen vähän (kuitenkin Kilpeläinen ja Nikunlassi 2006; Kilpeläinen 2016; Rätti ja Wallén 2017; Viinamäki ym.

2017). Vielä vähemmän tutkimusta on ihmisten alueella kokemasta turvallisuudesta ja/tai turvattomuudesta digitalisaatioon liittyen (kuitenkin Salminen 2019; Zojer 2019a). Tämän tutkimuksen teoreettisena viitekehyksenä toimivan inhimillisen turvallisuuden näkökulman arvo on sen kyvyssä tuoda yhteen sekä edellä mainitut tutkimuspolut ja kyberturvallisuustutkimus että yksilöiden ja yhteisöjen määrittelemät digitaalisen kehityksen mahdollisuudet ja uhkat. Tällä on vaikutusta siihen, millaisia sisältöjä digitaalinen turvallisuus voi saada.

Artikkeli koostuu johdannon jälkeen neljästä osasta. Ensin selvennän, mihin inhimillisen turvallisuuden viitekehyksestä nousevalla digitaalisen turvallisuuden käsitteellä artikkelissa viittaan. Tämän jälkeen käyn läpi digitalisaation ja kyberturvallisuuden käsitteet. Seuraavaksi esittelen Enontekiön tapaustutkimuksen tutkimusasetelman ja tutkimuksen tulokset. Viimeisessä osiossa tarkennan digitaalisen turvallisuuden käsitettä työpajakeskustelujen pohjalta. Tieto- ja kyberturvallisuudessa suojattaviksi kohteiksi ovat vakiintumassa tieto ja kriittinen infrastruktuuri tai yhteiskunnan elintärkeät toiminnot. Siksi käytän tässä inhimilliseen hyvinvointiin keskittyvässä analyysissa digitaalisen turvallisuuden käsitettä (Salminen 2018; Zojer 2019b). Käsite ohjaa huomion digitalisaation ihmisten arkipäivässä aikaansaamiin vaikutuksiin ja niihin liittyviin turvallisuuden ja turvattomuuden kokemuksiin. Koska digitaalisen turvallisuuden käsitteen sisältö määrittyy niissä ympäristöissä, joissa siihen liittyvää tutkimusta tehdään, ei Tunturi-Lapin tapaustutkimuksen löydöksiä voi yleistää muihin konteksteihin. Tutkimustapa on siirrettävissä erilaisiin ympäristöihin.

Inhimillinen turvallisuus, digitalisaatio ja kyberturvallisuus

Inhimillisen turvallisuuden näkökulmaan tukeutuen tarkoitan tässä artikkelissa digitaalisella turvallisuudella Enontekiön työpajoissa esiin nousseita, yhteiskunnan digitalisaatioon liittyviä tekijöitä, jotka joko parantavat arkipäivän hyvinvointia (vapaus johonkin, positiivinen turvallisuus) tai mahdollisesti heikentävät sitä (ja hyvinvointia heikentäviin tekijöihin vaikuttaminen negatiivisena turvallisuutena, vapautena jostakin) (esim. Hoogesen Gjørv 2012, 836). Hyvinvoinnin ja turvallisuuden suhde on läheinen: yksilöiden ja yhteisöjen hyvinvointi on tavoite, johon pyritään inhimillistä turvallisuutta vahvistamalla. Artikkelin näkökulmassa korostuu enontekiöläisten turvallisuuden kokemus (subjektiivinen turvallisuus), mutta se sisältää myös laajempia arvioita vallitsevasta turvallisuuden tilasta (objektiivinen turvallisuus); etenkin puhuttaessa toisista ihmisistä (ks. Wolfers 1952). Työpajoissa digitaalinen ja fyysinen toimintaympäristö sulautuivat puheessa toistuvasti yhteen: fyysisten toimien nähtiin vaikuttavan digitaalisessa ympäristössä (esimerkiksi satelliittien alas ampuminen) ja päinvastoin (esimerkiksi haukkuminen sosiaalisessa mediassa, mikä vaikuttaa kohteeksi joutuneen hyvinvointiin) (myös van Dijck 2013, 19; Junger, Montoya ja Overink 2017, 75–76).

Inhimillinen turvallisuus määritellään yleensä kahden tai kolmen vapauden kautta: vapaus pelosta ja vainosta (freedom from fear), vapaus puutteesta (freedom from want) sekä oikeus ihmisarvoiseen elämään (freedom from indignity) (Hampson 2008, 230–232; Tadjbakhsh ja Chenoy 2009, 17). Niin inhimillisen turvallisuuden puolestapuhujat kuin sen arvostelijat ovat erimielisiä siitä, mihin tutkimuksen ja politiikkatoimien kuuluisi kohdistua. Kapea-alaisesti voidaan vaatia keskittymistä ihmisten kohtaamaan väkivaltaan (joko suoraan tai rakenteelliseen; fyysiseen tai henkiseen), eli vapauteen pelosta ja vainosta. Laa-

jemmin kehykseen voidaan sisällyttää vapaus puutteesta, mikä tuo mukanaan tavoitteen päästä eroon niin luonnonmullistuksista kuin inhimillisestä toiminnasta johtuvasta puutteesta ihmisten ja yhteisöjen arkipäivässä. Laajimmillaan kyse on ihmisten vapauden ja itsensä toteuttamisen edistämisestä. (Esim. Kerr 2007, 95; Tadjbakhsh ja Chenoy 2009, 21.) Yksilöt ja yhteisöt toimivat tällöin myös turvallisuutensa ja siihen kohdistuvien uhkien määrittelijöinä.

Inhimillinen turvallisuus pohjaa perus- ja ihmisoikeuksiin. Näkökulman kehittämisessä 1990-luvulla oli kyse vastaamisesta valtavirran turvallisuusajattelussa tunnistettuun heikkouteen: turvallisuusagendalta puuttui ihmisten kokemus (Hoogesen Gjørv 2017, 107; Tadjbakhsh ja Chenoy 2009, 10). Yksilöiden kansalaisoikeudet sekä taloudelliset, sosiaaliset ja sivistykselliset oikeudet nähtiin vähintään yhtä vahvoiksi kuin valtioiden oikeudet (Fierke 2015, 156). Yksilöt ja yhteisöt voivat myös vaatia oikeuksiensa kunnioittamista – ei valtioiden kansalaisina vaan yksinkertaisesti ihmisinä (Brown ja Ainley 2009, 221–222). Valtioiden tunnistettiin voivan loukata kansalaistensa oikeuksia, minkä vuoksi arkipäivän turvallisuuden ja hyvinvoinnin tuli olla ensisijaista (Buzan ja Hansen 2009, 206; Kerr 2007, 92–93). Yksilöstä tuli se perusyksikkö, jonka turvallisuudesta tuli huolehtia – myöhemmin yhteisöjen oikeudet ovat vahvistuneet viitekehyksen sisällä. Turvattomuuden ja tyytymättömyyden vähentyminen johtaisi välillisesti yhteiskunnallisen turvallisuuden lisääntymiseen (Kerr 2007, 93, 96).

Moniselitteisyytensä vuoksi inhimillistä turvallisuutta on kritisoitu epämääräisyydestä, kyseenalaisesta toteuttamiskelpoisuudesta, kaiken turvallistamisesta ja liiallisesta tilannesidonnaisuudesta sekä taipumuksesta kolonialismiin. Lisäksi on nostettu esiin epäselvä suhde ihmisoikeuksiin. (Kerr 2007, 95–98, 103–104; Martin ja Owen 2010, 213; perusteellista yhteenvetoa kritiikistä ja siihen vastaamisesta ks. Tadjbakhsh ja Chenoy 2009.) Vuoden 1994 Inhimillisen kehityksen raportti, joka popularisoi inhimillisen turvallisuuden, jaotteli turvallisuuden yksilön ja yhteisön turvallisuuteen, taloudelliseen, poliittiseen ja terveyteen liittyvään turvallisuuteen sekä ruoka- ja ympäristöturvallisuuteen (UNDP 1994). Myös tämä sektorijako on nostattanut kritiikkiä, minkä vuoksi esimerkiksi Martin ja Owen (2010, 221) ehdottavat, että uhkalistauksen sijaan inhimillinen turvallisuus nähtäisiin kynnysarvona, jonka ylittäessään asia voi muuttua turvallisuusuhkaksi. Keskeistä uhkan määrittelylle olisi siten sen vakavuus. Vuoden 1994 raportti ei mainitse digitalisaatiota tai kyberturvallisuutta, mutta viittaa tietoon ja sen kontrollointiin, satelliitteihin, kommunikaation välittömyyteen, tietokoneisiin ja tietokoneverkkoihin sekä teknologisiin innovaatioihin (UNDP 1994, 2, 33–34, 70, 88.). Sana digitaalinen esiintyy ensimmäisen kerran vuoden 1999 raportissa kuvaamassa viestintäteknologian murrosta ja sen kauaskantoisia vaikutuksia sekä verkostoyhteiskunnan syntyä (UNDP 1999, 58). Kyber-etuliitettä käytetään samassa raportissa, valtavirran kyberturvallisuusajattelusta poiketen, kuvaamassa vähemmistöryhmien ja syrjäytettyjen mahdollisuutta löytää joukkovoimaa nettiyhteisöistä ja vastustaa oikeuksiensa polkemista (UNDP 1999, 59).

Digitalisaatio-käsitteenkään sisältö ei ole yksiselitteinen. Tässä artikkelissa tarkoitan sillä käytettävissä olevien televiestintäyhteyksien lisääntymisen ja niiden laadun parantumisen ohella laajempaa yhteiskunnallista muutosta, missä yhä useampi sosiaalisen elämän alue järjestyy uudelleen digitaalisten tieto- ja viestintäteknologioiden kasvavan käytön mukaan (Brennen ja Kreiss 2014; myös Latham ja Sassen 2005 Schoun ja Hjelholtin 2018, 9 mu-

kaan). Digitalisaatio haastaa ”kyseenalaistamaan olemassa olevat toimintatavat ja luomaan ne uudelleen”[13]. Se pureutuu syvälle yhteiskunnallisiin rakenteisiin ja muuttaa käytäntöjä eli totuttuja tapoja ajatella ja tehdä asioita. Suomessa valtionhallinto on aktiivisesti edistänyt digitalisaatiota 1990-luvulta alkaen (esim. Lilius 1997). Kehityskulun tunnistetut hyödyt liittyvät kustannustehokkuuteen, ajasta ja paikasta riippumattomuuteen, läpinäkyvyyden paranemiseen, palvelutarjonnan lisääntymiseen ja ympäristöystävällisyyteen (esim. Lapin liitto 2007, 22; 2013, 4, 23; 2016, 13). Yhteiskunnallinen muutos näkyy työn muutoksena, palvelutarjonnan uudelleen järjestämisenä, ympärivuorokautisuutena, laitteiden ja ohjelmien etäkäyttönä sekä tiedon saatavilla olemisena lisääntyvässä määrin (esim. Lapin liitto 2013, 4–5; 2016, 8–13).

Digitalisaatiopuheessa ja -käytännöissä tieto- ja viestintäteknologia mielletään usein neutraaliksi, kaikkien elämään jokseenkin yhtäläisesti ja positiivisesti vaikuttavaksi globaaliksi muutosvoimaksi (Carr 2016, 22–23; van Dijck 2013, 6; Schou ja Hjelholt 2018, 6, 10; Webster 2006, 11–12). Todellisuudessa ihmisten suhde teknologiaan vaihtelee yhteiskunnittain kietoutuen osaksi monimutkaisia arvoihin, asenteisiin, uskomuksiin, instituutioihin ja käytäntöihin liittyviä historiallisia kerrostumia (ks. Carr 2016; Hui 2016; Wheeler 2013). Janssonin ja Sihvosen (2018, 1–2) sanoin teknologia ei ole vapaa ”poliittisista ideologioista, kansallisvaltioiden päämääristä tai kaupallisista intresseistä”. Se kehittyy arkipäivän käyttötarpeiden mukaan samalla muokaten näitä tarpeita ja sitoen välineiden avulla tapahtuvan sosiaalisen vuorovaikutuksen osaksi yhteiskunnan institutionaalista rakennetta. Teknologia ja sen käyttäjät, ja siten myös teknologia ja yhteiskunta, rakentuvat vuorovaikutuksellisissa prosesseissa. (Van Dijck 2013, 5–6; Seppänen & Väliverronen 2012.) Teknologianeutraliteetin olettamus johtaa kuitenkin tilanteeseen, jossa otaksutaan, että esimerkiksi yksilöt, yhteisöt, alueet, ikäryhmät tai ammattiryhmät kohtaavat digitalisaation samoista lähtökohdista (Pare 2005, 85, 88). Tunnistettujen erityisryhmien tarpeisiin on Suomessa pyritty vastaamaan 2000-luvun alkupuolelta valtakunnallisilla esteettömyys-/saavutettavuusohjelmilla[14], mutta politiikkalinjoja saatetaan silti vetää perehtymättä esimerkiksi kehityskulun alueellisiin erityispiirteisiin. Alueellisten tietoyhteiskunta- ja digistrategioiden valmistelussa on kuultu paikallisia julkishallinnon edustajia, yrityksiä ja organisaatioita sekä asukkaita internetkyselyiden ja työpajojen avulla (esim. Lapin liitto 2007, 5, 17–19; 2013, 34). Digitalisaatio ja siihen liittyvät arkipäivän turvallisuuskysymykset ovatkin aina aikaan ja paikkaan sidoksissa (Salminen ja Hossain 2018; Schou ja Hjelholt 2018, 12, 86–88; Webster 2006, 12).

Digitalisaatioon liittyviä turvallisuuskysymyksiä on yleensä tarkasteltu teknologianeutraalisti tietoturvallisuudessa ja kyberturvallisuudessa, jotka määritellään monin tavoin eikä niiden välinen suhde ole selvä. Suomessa tiedosta tuli yhteiskunnallisen turvaamisen kohde vuoden 2004 kansallisessa tietoturvastrategiassa ja kybertoimintaympäristöstä vuoden 2013 kyberturvallisuusstrategiassa. Koska tietoturvallisuus voidaan sisällyttää kyberturvallisuuteen, tarkastelen ainoastaan jälkimmäistä käsitettä. Kyberturvallisuudessa tavoitteena on varmistaa (1) tiedon luottamuksellisuus, eheys ja saatavuus teknisin, hallinnollisin ja koulutuksellisin keinoin (Brotby 2009, 6; Singer ja Friedman 2014, 35–36; 70–71; vrt. Lewis 2015, 146) sekä (2) kriittiseksi määritellyt infrastruktuurit, yhteiskunnan elintärkeät toiminnot tai yleisemmin digitalisoituvan yhteiskunnan toimivuus, mukaan lukien esimerkiksi ihmisoikeuksien toteutuminen ja demokratia. (Kramer, Starr ja Wentz 2009; Lewis 2015; Singer ja Friedman, 2014.) Kyberturvallisuuden merkitys nousee tarpeesta turvata digitalisaation

avaamat, tavoiteltaviksi arvotetut mahdollisuudet. Informaatioinfrastruktuurin haavoittuvuudet, sen globaalius, kompleksisuus ja kaikkialla läsnä oleminen, sekä inhimillinen laitteiden käyttö tekevät toimintaympäristöstä epävarman ja osittain ennakoimattoman. (Lewis 2015, 93–194; Limnéll, Majewski ja Salminen 2014, 15, 63–71, 158.)

Tässä artikkelissa pyrin Enontekiön tapaustutkimuksella laajentamaan ja syventämään kyberturvallisuusymmärrystä siten, että siihen sisältyvät teknisten, hallinnollisten (ml. koulutukselliset) ja strategisten (valtion/yhteiskunnan turvallisuus) turvallisuuskysymysten ohella yksilöiden ja yhteisöjen arkipäivässään kohtaamat, kiihtyvästä digitalisaatiosta juontuvat epävarmuudet. Kyberturvallisuudessa ihmisten arkipäiväiset, onnistuneesta tai epäonnistuneesta tiedon, infrastruktuurin tai elintärkeiden toimintojen suojaamisesta johtuvat tilanteet nähdään yleensä toisen tai kolmannen aallon vaikutuksiksi. Digitaalinen turvallisuus taas on kiinnostunut juuri näistä inhimillisistä vaikutuksista ja nostaa yksilöt ja yhteisöt ensisijaisiksi suojaamisen kohteiksi. (Ks. Salminen 2019; Salminen ja Hossain 2018). Näkökulman puuttuminen on tunnistettu heikkous kyberturvallisuustutkimuksessa (Dunn Cavelty 2014), vaikka puheenvuorot ”ihmiskeskeisestä kyberturvallisuudesta” ovat lisääntyneet niin akatemiassa ja liike-elämässä (Deibert 2018; Renaud ja Flowerday 2017; Zimmermann ja Renaud 2019) kuin kansainvälisissä järjestöissä, kuten Yhdistyneet kansakunnat[15] ja Taloudellisen yhteistyön ja kehityksen järjestö[16]. Ihmiskeskeinen turvallisuus voi puheenvuoroissa tarkoittaa hyvinkin eri asioita, kuten ihmisoikeuksista lähtevää kyberturvallisuuden tarkastelua (Deibert 2018) tai huomion kiinnittämistä ihmiseen kyberturvallisuuden heikoimpana lenkkinä (Anwar ym. 2017; Yan ym. 2018).

Tutkimusasetelma

Tämän tapaustutkimuksen kohteena on enontekiöläisten kokemus digitalisoituvan arkipäivän turvallisuudesta. Koska empiiristä tutkimusta aiheesta Euroopan pohjoisilla alueilla on vähän, pidettiin marraskuussa 2018 kaksi world café -metodia soveltavaa työpajaa, yksi kuntakeskus Hetassa ja toinen Suomen, Ruotsin ja Norjan rajaseudulla Kilpisjärvellä[17]. Metodi valittiin Vaasan yliopiston johtamassa tutkimushankkeessa vuonna 2016 pidettyjen turvallisuuskahviloiden innoittamana (Raisio ym. 2017). Työpajoihin olivat tervetulleita kaikki keskustelutilaisuuksien tematiikasta, ”Arjen digipalvelut Enontekiöllä”, kiinnostuneet. Enontekiöläisiä edustavat työpajoihin saapuneet henkilöt, vaikkei kattavaa otantaa kuntalaisten kokemuksista näin saada[18].

Työpajoihin osallistui neljästä kymmeneen henkilöä (kaikkiaan 16 osallistujaa), osan tullessa myöhemmin tai joutuessa lähtemään keskustelun ollessa meneillään. Osallistujien vaihtuvuuden vuoksi joukkoa ei tapahtumissa jaettu pienryhmiin, vaan keskustelu käytiin yhdessä ryhmässä. Aluksi osallistujille esiteltiin lyhyesti tutkimushanke, tutkija, kerättävän tiedon käyttötarkoitukset ja säilyttäminen tutkimushankkeen jälkeen. Lisäksi osallistujilta pyydettiin lupa keskustelujen nauhoittamiseen ja kerrottiin tutkimuksessa ylläpidettävästä anonymiteetista. Keskusteluaika tapahtumissa oli reilut kaksi tuntia. Aikaa ei kontrolloitu, vaan tilaisuus päättyi, kun osallistujilla tai vetäjällä ei ollut uutta sanottavaa. Keskustelua käytiin väljästi viiden tutkimuskysymysryhmän pohjalta, jokainen sai tuoda ajatuksensa esiin silloin kuin ne mieleen nousivat sen sijaan, että olisi pitäydytty tarkasti etukäteen mää-

rätyissä rajoissa. Työpajojen tavoitteena oli luoda ajassa ja paikassa kiinni oleva diskurssi valitusta aiheesta, jossa tavalla tai toisella käytäisiin kysymykset läpi. Metodilla kyettiin lyhyessä ajassa keräämään temaattista analyysia varten riittävän monipuolinen aineisto, joka kertoo yksilöiden näkemysten lisäksi myös yhteisöllisistä normeista ja odotuksista. (Gibson ja Brown 2009, 86–89; Hennink, Hutter ja Bailey 2011, 135–168.)

Anonymiteetin vuoksi työpajan osallistujista ei kerätty taustatietoja eikä aineistoa käsiteltäessä tehty eroa puhujien suhteen tai sen suhteen, kummassa työpajassa jokin asia nousi esiin tai tuli sanotuksi. Tämä oli tärkeää, koska tapaustutkimus tehtiin vähäväkisellä paikkakunnalla, missä kaikki tietävät toisensa ja yksittäiset puhujat saattavat olla tunnistettavissa hyvinkin hajanaisten tietojen perusteella. Analyysiosiossa olen raportoinut ainoastaan työpajojen merkittävät erot. Nauhoitetut keskustelut litteroitiin helmikuussa 2019 opiskelijatyönä, jolloin myös työn tehnyt opiskelija allekirjoitti vaitiolositoumuksen.

Työpajakeskusteluja ohjasi viisi tutkimuskysymysryhmää (taulukko 1), jotka oli tulostettu useille A4-papereille ja jotka olivat osallistujien nähtävillä koko keskustelun ajan.

Taulukko 1. Työpajakeskusteluita ohjanneet tutkimuskysymysryhmät.

I	Miten käytät tietoteknologiaa arkipäivässäsi? Miten haluaisit sitä käyttää? Miten et haluaisi (joudut käyttämään)? Mitä sähköisiä palveluita kaipaisit? Mistä syystä ja mitä varten? Mihin palveluihin olet tyytyväinen?
II	Mitä elämänalueita tietoteknologia on muuttanut ja mitä ei? Millaiseen tulevaisuuden kehitykseen olisit tyytyväinen? Millaista kehitystä et halua?
III	Mitkä tekijät edesauttavat toivottua kehitystä ja mitkä haittaavat sitä? Miten edellisiä tekijöitä voitaisiin tukea ja jälkimmäisten tekijöiden vaikutusta vähentää?
IV	Pystytkö vaikuttamaan alueen kehitykseen? Jos kyllä, miten? Jos ei, miksi ei? Miten mahdollisesti haluaisit vaikuttaa? Mitä muuttaisit?
V	Mikä on valtion, alue-/paikallishallinnon, yritysten, järjestöjen, yhteisöjen ja yksilöiden rooli arkipäivän turvallisuuden ja luottamuksen luomisessa ja ylläpitämisessä?

Tekstiaineisto jaoteltiin temaattisesti, eli siitä nostettiin esiin keskeisimmät asioiden väliset suhteet, yhtäläisyydet ja erot, joiden katsottiin rajaavan teemoja (Gibson ja Brown 2009, 127–129; Gomm 2008, 244). Analyysissa ei pyritty toistamaan enontekiöläisten sanamuotoja vaan teemoittelemaan digitalisaatioon liittyviä kokemuksia, jotka nousivat edellä mainittujen kysymysten ohjaamassa keskustelussa esiin tai jotka olivat tutkimuksen teoreettisen viitekehyksen ohjaamina kysymyksiin sisäänkirjoitettuja. Työpajojen keskustelut ovatkin aina vetäjän ja niihin osallistuvien keskisiä vuorovaikutustilanteita, joissa konstruoidaan valittua aihetta ja joihin ryhmädynamiikka vaikuttaa, mikä mahdollistaa uusien, etukäteisodotuksista poikkeavien teemojen esiin tulemisen. (Guest, MacQueen ja Namey 2012, 50; Gibson ja Brown 2009, 88–89, 130–133; Gomm 2008, 244; Hennink, Hutter ja Bailey 2011, 136.) Teemoittelun jälkeen selvitettiin, mitkä teemat liittyvät tai eivät liity toisiinsa. Samoin selvitettiin, esiintyvätkö teemat aineistossa positiivisessa vai negatiivisessa valossa, neutraaleina tai mahdollisesti eri painotuksin eri yhteyksissä. (Vrt. Gomm 2008, 244–245, 249.) Temaattista analyysia on kritisoitu yksilöiden elämänkokemusten koostamisesta abstraktioiksi, jotka eivät välitä samaa tietoa kuin ihmisten kertoma (Gibson ja Brown 2009, 129;

Hennink, Hutter ja Bailey 2011, 138). Vähäväkisellä paikkakunnalla tehdyssä tutkimuksessa tällä on kuitenkin oma arvonsa tutkimukseen osallistuneiden yksilöiden tunnistettavuuden vähentämisessä.

Digitaalinen turvallisuus Tunturi-Lapissa

Tutkimusasetelmasta johdetut rakenteelliset teemat[19] (n=5) (taulukko 2) sisältyivät tutkimuskysymyksiin.

Taulukko 2. Tutkimusasetelmasta johdetut rakenteelliset teemat.

I	Tietoteknisten laitteiden käyttö
IIa	Digitalisaatioon liittyvät inhimillisen turvallisuuden mahdollisuudet
IIb	Digitalisaatioon liittyvät inhimillisen turvallisuuden haasteet
III	Toivotunlaista digitaalista kehitystä edistävät tekijät ja sen esteet
IV	Yksilön vaikutusmahdollisuudet digitaaliseen kehitykseen
V	Eri toimijoiden roolit digitaalisen turvallisuuden tuottamisessa

Työpajakeskusteluista nousevat teemat[20] olivat keskustelukohtaisia, mutta analyysissa olen koonnut ne yhteen. Teemat (n=31) ja niiden sijoittuminen rakenteellisten teemojen alle on esitetty taulukossa 3 liitteessä 1. Analyysissa olen järjestänyt keskusteluista nousevat teemat rakenteellisten teemojen alle siten, että ne voivat keskustelusisältöjensä vuoksi esiintyä useamman rakenteellisen teeman alla. Tässä käsittelen vain keskustelusisältöjä, joissa määriteltiin arkipäivän digitaalista turvallisuutta Tunturi-Lapissa. Työpajakeskustelijat eivät välttämättä käyttäneet turvallisuuden sanastoa vaan saattoivat puhua esimerkiksi arkipäivän hyvinvointiin liittyvistä tekijöistä. Inhimillisen turvallisuuden laajaan näkökulmaan sisältyvät materiaalinen ja henkinen hyvinvointi sekä mahdollisuus itsensä toteuttamiseen, joten olen analyysissa ”kääntänyt” keskustelusisältöjä inhimillisen turvallisuuden ”kielelle”. Keskustelusisällöistä nostan esiin myös selviytymisstrategioita, joita enontekiöläiset hyödyntävät digitaalisuuden haasteissa.

Tietoteknisten laitteiden käyttö

Enontekiöläisillä oli käytössään lukuisia tietoteknisiä laitteita, joista puhelin oli monelle keskeisin. Se toimi tietovarastona, tiedon hankkimisen välineenä, yhteydenpitovälineenä sekä työ- ja apuvälineenä. Lisäksi se oli turvaväline, jolla sai tarpeen tullen hälytettyä apua etäisyyksien taakse, minkä vuoksi oli huolehdittava puhelimen akun kestosta tai sen lataamismahdollisuudesta, pidettävä puhelin lämpimänä talvipakkasilla sekä tiedettävä televiestintäverkon katvealueet. Osa työpajaosallistujista oli sitä mieltä, etteivät he puhelimen turvavälinetehtävän vuoksi voisi laittaa sitä äänettömälle tai jättää vastaamatta soittoihin. Osa koki, että vapaaehtoinen luopuminen puhelimesta ja tavoitettavissa olemisesta ajoit-

tain teki hyvää. Tavoitettavuus siten lisäsi turvallisuutta ja turvallisuuden tunnetta, mutta jatkuvasti tavoitettavissa olemisen ja välittömästi viesteihin vastaamisen odotukset kuormittivat. Kuten analyysissa myöhemmin ilmenee, puhelimen käyttämiseen rakentuva ristiriita hyödyllisen ja haitallisen tavoitettavuuden välillä sisältyy digitaaliseen turvallisuuteen laajemminkin: digitalisaatio avaa uusia mahdollisuuksia hyvinvoinnin lisäämiseen (positiivinen turvallisuus), mutta myös sen vähenemiseen (ja tämän vähenemisen vastaisiin toimiin negatiivisena turvallisuutena) (ks. Hoogesen Gjørv 2012).

Vanha puhelin oli työpajoissa kerrotun mukaan turvallisuusriski, sillä siihen ei saanut ohjelmistopäivityksiä ja tiedon hallittu siirtäminen vanhalta laitteelta uuteen ja tuhoaminen luotettavasti oli vaikeaa. Edelleen toimivan puhelimen uusiminen tuntui turhalta ja lisäsi elektroniikkajätteen määrää. Puhelimen häiriöttömään toimintaan ei myöskään voinut luottaa, sillä enontekiöläisillä oli kokemuksia pitkistä televiestintäverkon häiriöistä, joiden aikana he olivat joutuneet etsimään toisen operaattorin liittymän omistajaa tai ajamaan Norjan tai Ruotsin puolelle soittamaan. Pitkien häiriöiden takia oli ehkä havahduttu omaan puhelinriippuvuuteen tai laitteen tuottamaan väärään turvallisuuden tunteeseen. Puhelimen merkitys arkipäivän monitoimilaitteena linkittyy kahteen glokaaliin järjestelmään: sähkö- ja televiestintäverkkoihin ja ympäristöön. Sosiaalisen median alustojen analyysissaan van Dijck (2013, 21) ehdottaa alustojen tarkastelua mikrojärjestelminä, jotka toisiinsa kytkettyinä muodostavat ekosysteemin. Puhelin voidaan myös ymmärtää mikrojärjestelmäksi, jonka turvallisuuden ja/tai turvattomuuden ulottuvuudet tulevat esiin tarkasteltaessa sitä osana sähköja televiestintäverkkoja. Kuten työpajoissa tuotiin esiin, puhelin toimi turvavälineenä niin kauan kuin sen käyttäjä oli toimivien televiestintäverkkojen kattavuusalueella. Lisääntyvä elektroniikkajäte taas on osa globaalia ympäristöongelmaa.

Eri ikäryhmien erilaiset tavat käyttää tietoteknisiä laitteita sekä eriasteiset ohjauksen ja neuvonnan tarpeet nousivat työpajakeskusteluissa toistuvasti esiin. Nuorille tietotekniikan ja sen avaamien mahdollisuuksien arveltiin olevan hyvinvointia lisäävä tekijä muun muassa sosiaalistumisen ja ajanvieton kannalta, vaikka samalla saatettiin todeta lasten olevan digiriippuvaisia jo varhaisella iällä. Digiriippuvuuden myönnettiin vaivaavan myös aikuisia. Erityisen huolissaan oltiin yksinäisten vanhusten kyvystä pärjätä ja pysyä teknologian nopeassa kehityksessä mukana, sillä heillä ei ole nuorempia sukulaisia tai tuttavia auttamassa asioiden hoitamisessa. Digitalisaatiota pidettiin yksilöitä ja yhteisöjä, myös kuntia, eri tavoin kohtelevana kehityksenä, jonka erityispiirteisiin pitäisi kiinnittää huomiota niin yhteiskunnallisessa ohjauksessa kuin tietoteknisiä laitteita ja digitaalisia palveluita toimittavissa yrityksissä. Digitaalinen turvallisuus kietoutuu tällöin osallisuuteen ja perusoikeuksien toteutumiseen sekä yksilöiden, yhteisöjen ja alueiden tarpeiden erilaisuuteen. Digitalisaation edetessä ei ole riittävästi pohdittu, miten kehitys vaikuttaa perusoikeuksien toteutumiseen tai mitä ne digitalisoituneessa yhteiskunnassa tarkoittavat. Samaa keskustelua käydään ihmisoikeuksien osalta (esim. Wagner, Kettermann ja Veith 2019).

Enontekiöllä etäisyydet edesauttavat digitalisaation näkemistä positiivisessa valossa. Työpajoissa todettiin, että paikkakunnalla elettiin ”sen verran syrjässä” ja elämäntavan tietoisesti valinneina, että tietoteknisten laitteiden käytöllä pystyi huomattavasti helpottamaan arkipäiväänsä, mikä tarkoitti ennen kaikkea matkustamistarpeen vähenemistä. Suhtautuminen digitalisaatioon oli positiivisempaa Kilpisjärvellä kuin Hetassa, mikä selittynee arjen kokemusten erilaisuudella: Kilpisjärvellä digitalisaatio on tuonut palvelut lähemmäksi, kun

taas Hetassa fyysisten palvelupisteiden korvaaminen digitaalisilla on vähentänyt asioinnin henkilökohtaisuutta. Etäisyyksien ja paikallistuntemuksen teema esiintyi työpajoissa muun muassa pakkona käyttää digitaalisia palveluita ja tilata hyödykkeet netin kautta, hankaluutena tulla toimeen ilman tietoteknisiä laitteita ja digitaalisia palveluita, kouluttautumis- ja harrastusmahdollisuuksien paranemisena, muutoksina työnkuvassa, monipuolisina mahdollisuuksina yhteydenpitoon, mutta myös inhimillisyyden vähenemisenä asioinnissa, mikä pahimmillaan vähensi luottamusta asioiden etenemiseen ja lisäsi turvattomuuden tunnetta.

Digitalisaatioon liittyvät inhimillisen turvallisuuden mahdollisuudet

Yksi digitalisaation suurimmista hyödyistä Enontekiöllä koskee asiointia. Monet digitaaliset palvelut toimivat hyvin ja alkujaan pankkiasiointi on voinut olla syy tietokoneen hankkimiseen. Ajasta ja paikasta riippumattoman asioinnin lisäksi digitalisaatio parantaa ennakoimisen mahdollisuuksia, mikä taas on yksi turvallisuuden osatekijöistä (ks. Päläs ja Salminen 2019, 328). Työpajoissa kerrotun mukaan asiointireissuja varten netistä tarkistettiin liikkeiden ja palveluiden sijainnit ja aukioloajat. Palvelut pyrittiin löytämään mahdollisimman läheltä, tapaamisajat varaamaan etukäteen ja varmistamaan puhelinsoitolla. Reitit suunniteltiin sää-, liikenne- ja aikataulutietojen mukaan. Ennakoimisen ja netin kautta tilaamisen teemat liittyvät toisiinsa, sillä ennakointia tarvittiin hyödykkeiden saatavuuden varmistamiseksi: päivittäisiä ruoka- ja sekatavaraostoksia lukuun ottamatta kaikki tarpeellinen oli Enontekiölle tilattava. Tilaukset tehtiin isoina erinä, jotta hyödykkeet toimitettiin kotiovelle, mikä helpotti etenkin autottomien arkipäivää. Mikäli tämä ei onnistunut, oli edessä matka Kilpisjärveltä yli sadan kilometrin päähän tai keskuksissa töissä käyvien naapureiden vaivaaminen. Huolena oli, että netistä tilaaminen näivettäisi loputkin paikalliset palvelut. Digitalisaation avaamat mahdollisuudet parantavat inhimillistä turvallisuutta arkipäivässä. Parhaimmillaan ne lisäävät valinnanvapautta ajankäyttöön ja vapauttavat epävarmuudesta lisäämällä saatavilla olevaa tietoa, mikä esimerkiksi lisää tilausten toimitusvarmuutta ja liikenneturvallisuutta.

Ennakoimisen teemaan liittyvät osittain myös paikalliset sovellukset ja sosiaalisen median käyttötavat. Työpajoissa mainittiin Facebookin Rekat ravissa valtatie 21 -ryhmä, jossa jaettiin tietoa valtatien kelitilanteesta ja onnettomuuksista, sekä Porokello-sovellus, johon ammattiautoilijat päivittivät porohavaintojaan ja joka hälytti tielläliikkujan tullessa aiemman havainnon kohdalle[21]. Poromiehillä ja -naisilla oli käytössään paikkatietopohjainen sovellus, jolla pystyi seuraamaan porotokkien liikkumista. Kehitteillä oli myös sovellus, joka mahdollistaisi poron omistajatietojen näkemisen puhelimen koodinlukijalla suoraan piltasta[22]. Kyläyhteisön hyvinvoinnin kannalta merkittäviksi mainittiin sosiaalisen median alustoille siirtyneet kylien ilmoitustaulut, joilla tiedotettiin muun muassa tulevista tapahtumista. Kunnan digitalisoiduista palveluista oli kahtalaisia kokemuksia: osa koki palvelut vaikeakäyttöisiksi, osa hyvinkin käyttäjälähtöisiksi. Paikallisilla palveluilla, sovelluksilla ja sosiaalisen median käyttötavoilla vastataan tarpeisiin, joita ei valtakunnallisesti tunnisteta tai joiden katsotaan koskevan niin pientä joukkoa, ettei niiden valtakunnalliselle kehittämiselle ole tarvetta, kehittäjää tai riittävää paikallistuntemusta. Paikallisiin tarpeisiin räätälöidyillä ratkaisuilla tuetaan inhimillisen turvallisuuden eri sektoreita, kuten edellä kerrotuissa esimerkeissä taloudellista turvallisuutta, liikenneturvallisuutta ja yhteisöturvallisuutta sekä

perusoikeuksia, joiden toteutumiseksi kunnalla on velvollisuus laissa määriteltyjen palveluiden järjestämiseen (myös Zojer 2019a).

Avunsaanti nousi esiin digitalisaation mahdollisuuksien yhteydessä. Puhelimella sai avun soittamisen ohella otettua potilaasta kuvan lääkärille lähetettäväksi ja ensiapuohjeiden pyytämiseksi. Hätätilanteissa ambulanssin saapuminen Enontekiölle saattaa kestää, joten paikallaolijoiden antama ensiapu on ensisijaista. Työpajakeskustelijoiden mukaan sosiaalisessa mediassa olisi potentiaalia inhimillisen turvallisuuden edistämiseen, mikäli alustoille saataisiin kehitettyä kanava, jonka kautta henkisesti pahoinvoivien viesti välittyisi auttaville tahoille. Palvelun esikuvana toimisi 112 Suomi -sovellus. Avuntarpeen odotettiin lisääntyvän, minkä vuoksi olisi tärkeää keksiä keinoja digitaalisuuden hyödyntämiseksi. Sosiaalisen median mainittiin jo nyt palvelevan vertaistukiryhmänä (joita paikkakunnalla ei muuten ole) tai yhteisönä, josta voi löytää mielenkiinnon kohteidensa mukaisia ”kuplia” ja jossa koordinoidaan vapaaehtoisapua (myös Vainikka ja Harju 2019). Avunsaannin yhteydessä valvontamahdollisuuden nähtiin lisäävän turvallisuutta. Yhteydenpidolla voitiin esimerkiksi päivittäin tarkistaa vanhemman sukulaisen vointi. Kunnassa oli toteutettu kotona asumista tukeva Toimiva kotihoito Lappiin -hanke[23], jossa kuvapuhelinten ja anturitolppien avulla oli seurattu asiakkaiden vointia ja aktiivisuutta heidän turvallisuutensa lisäämiseksi. Kokemuksen mukaan laitteet eivät kuitenkaan aina toimineet, asiakkailla oli vaikeuksia käyttää kosketusnäytöllistä puhelinta ja laitteiden asentaminen sekä henkilöstön kouluttaminen vaati resursseja. Pitkät etäisyydet, väestön ikärakenne, vaihtelevat digitaidot, kunnan rajalliset resurssit ja digitalisaation vaillinainen taipuminen tarpeisiin rajoittavat digitaalisen kehityksen mahdollisuuksien hyödyntämistä inhimillisen turvallisuuden parantamiseksi.

Digitaaliset terveyspalvelut ja virtu.fi-palveluportaali[24] todettiin työpajakeskusteluissa toimiviksi ja terveyteen liittyvää turvallisuutta lisääviksi. Portaalin kautta voi käyttää muun muassa kanta.fi-palvelua. Palvelussa oli havaittu viivettä tietojen päivittymisessä ja eteenpäin siirtymisessä, käyttökatkoja ja henkilötietojen sekaantumista. Tietojen sekaantumisen syyksi arvioitiin tietokannan käyttäjät, ei niinkään tekniikka, ja tietojen korjaamista oli voinut pyytää palveluntarjoajalta. Näkemys tietokannan käyttäjistä teknisiä haavoittuvuuksia suurempana turvallisuusuhkana on samansuuntainen valtavirran kyberturvallisuusajattelun kanssa, jossa yksilö inhimillisine heikkouksineen tulkitaan usein uhkaksi (ks. Päläs ja Salminen 2019, 320). Terveystietojen yhteydessä uhka liittyy tietosuojaan, mutta myös mahdollisuuteen saada väärä diagnoosi tai lääkitys. Inhimillisen turvallisuuden näkökulmasta on tärkeää tunnistaa yksilö turvallisuuden tuottajaksi, joka omalla toiminnallaan voi parantaa omaa ja muiden turvallisuutta digitaalisessa toimintaympäristössä (esim. Päläs ja Salminen 2019). Työpajoissa henkisen hyvinvoinnin osalta ihmisten lisääntynyt kärsimättömyys, ”someahdistus” ja ”nettiriippuvuus”, keskittymiskyvyn heikentyminen sekä kynnyksen madaltuminen pahan olon purkamiseen muihin ihmisiin nähtiin seurauksiksi vaatimuksesta välittömään reagointiin, kasvottomuudesta ja ”somehäiriköinnin” helppoudesta. Digitalisaation vaikutus terveyteen liittyvään turvallisuuteen onkin kaksijakoinen: se parantaa mahdollisuuksia vuorovaikutukseen ja tuo terveyspalvelut lähemmäs asiakkaita, mutta samalla se lisää kiirettä, vaatii palveluiden käyttäjiltä uusia taitoja ja altistaa yksilöt ja yhteisöt haitallisellekin vuorovaikutukselle.

Pelaamisesta puhuttiin työpajoissa myönteisesti. Se oli lapsille ja nuorille tapa sosiaalistua ja piti heidät pois kylältä ”resuamasta”. Samalla kielitaito kehittyi. Vaikka pelaamista oli

aiemmin väheksytty, puhuttiin siitä nyt urheiluna tai jopa ammattina. Kaikkiaan digitalisaatio oli monipuolistanut harrastusmahdollisuuksia Enontekiöllä, mikä lisäsi inhimillistä hyvinvointia. Muun muassa kansalaisopistojen verkkokurssit ja virtuaaliset jumpat, kirjaston palvelut, arkistojen digitoiminen, sosiaalisen median harrastusryhmät, seurakunnan palvelut ja äänikirjat mainittiin hyvinä digitaalisina tuotteina ja palveluina. Lehtiä – niin kotimaisia kuin naapurimaiden – voi lukea aiempaa laajemmin digitoinnin ansiosta. Kotoa käsin voi kouluttautua aikaisempaa pidemmälle tai osallistua esimerkiksi ammatillisiin valmennuksiin. Kilpisjärvellä oppilaat olivat voineet 1990-luvulta alkaen jatkaa kylän koulussa yläasteen loppuun etäopetuksen ansiosta. Nykyisin etäopetusta toteutettiin myös Kilpisjärveltä muun muassa saamen kielillä. Monitoimitalon palo vuonna 2015 tarkoitti digiloikkaa taaksepäin, sillä monet käytössä olleet laitteet ja ohjelmat tuhoutuivat ja niitä oli resurssipulassa korvattu opetuskäyttöön soveltumattomilla välineillä. Lapsille ja nuorille mahdollisuus koulunkäyntiin ilman pakkoa muuttaa pois kotoa varhaisella iällä tai viettää tunteja koulukuljetuksessa päivittäin on parhaimmillaan vakautta ja turvallisuutta arkipäivään tuova tekijä.

Digitalisaation kerrottiin muuttavan työnkuvaa, mikä näkyi tietoteknisten laitteiden käyttönä, etätyömahdollisuuksina, etäkokouksina ja työtehtävien automatisointina. Parhaimmillaan digitalisaatio oli mahdollistanut valtakunnallisen asiantuntijaverkoston hyödyntämisen viranomaispäätösten tekemisessä. Paikalliskonttorin ruuhkauduttua tehtäviä oli siirretty muihin konttoreihin, jotta asiakkaita koskevat päätökset saatiin tehtyä määräaikojen puitteissa. Monen asiakkaan kohdalla kysymys oli taloudellisesta turvallisuudesta. Etätyö nähtiin suotavana kehityksenä ilmansaasteiden ja matkakulujen vähenemisen vuoksi. Sitä pidettiin kuitenkin raskaana työmuotona, jossa käytössä olevien laitteiden määrä lisääntyy. Etätyössä on siis olemassa kynnys, jonka ylittämisen jälkeen ajasta ja paikasta riippumaton, vapauttava työnkuva muuttuu raskaaksi koko ajan töissä olemiseksi ja alkaa heikentää hyvinvointia. Kaikkiaan digitalisaatio voi Enontekiöllä vähentää etäisyyksien, elämäntavan, maantieteellisten olosuhteiden, väestön sosioekonomisten asemien ja taloudellisten paineiden vaikutusta arkipäivässä. Osa muutoksista lisää inhimillistä turvallisuutta – ja parantaa taloudellisten, sosiaalisten ja sivistyksellisten oikeuksien toteutumista – mutta osa aiheuttaa lisähaasteita, joita käyn lähemmin läpi seuraavaksi.

Digitalisaatioon liittyvät inhimillisen turvallisuuden haasteet

Sähkö- ja televiestintäverkkojen luotettavuus on haaste arkipäivän turvallisuudelle Tunturi-Lapissa. Työpajaosallistujilla oli kokemusta pitkistä sähkökatkoista ja niiden seurauksena syntyneistä tai muista syistä johtuneista televiestinnän häiriöistä. Pitkä televiestintäliikenteen katko oli kertaalleen koettu vaaratilanteeksi, koska yhteyttä ei ollut saanut mihinkään. Osallistujat kertoivat, että viestinnän luotettavuutta lisäävästä kiinteästä valokuituverkosta puhuttiin kylillä paljon muun muassa Kuitua pohjoiseen ja Kuitu kylässä -hankkeiden[25] yhteydessä. Mobiiliverkon seuraavan sukupolven toimivuudesta oltiin huolissaan, koska nykyisilläkään yhteyksillä netti ei kaikkialla toiminut riittävän hyvin ja linkkimastojen määrää pitäisi lisätä. Mobiiliyhteyksien huomautettiin parantuneen viime vuosina ja katvealueita olevan entistä vähemmän – toiveissa oli, että loputkin paikattaisiin etenkin matkailun ja pelastustoimen vuoksi.

Sähkö- ja televiestintäverkkojen alueellinen toimivuus asettaa yksilöt ja yhteisöt erilaisiin asemiin digitalisaatiossa ilman, että he kykenevät asiaan vaikuttamaan. Verkot rakennetaan, niitä ylläpidetään ja niiden vika- ja häiriösietoisuutta parannetaan valtakunnallisista lähtökohdista, jolloin harvaan asuttujen alueiden tarpeet eivät ole tärkeysjärjestyksessä ensimmäisinä (esim. Salminen ja Hossain 2018). Yhteyksiä kehitetään keskuksista kohti syrjäseutuja ja yhteiskunnan elintärkeiden toimintojen kannalta keskeisten verkkojen toimivuus pyritään turvaamaan, jotta laajamittaista häiriötilannetta ei pääse syntymään (esim. Lehto ym. 2018). Alueellista epätasa-arvoisuutta on tasattu valtion ja Euroopan unionin tukitoimilla, mutta teknologian kehittyessä tukitarve säilyy. Enontekiöllä kerrottiin asuvan henkilöitä, joilla ei ollut lainkaan yhteyksiä kotonaan. Heidän osallisuudestaan ja perusoikeuksiensa toteutumisesta digitalisoituvassa yhteiskunnassa oltiin työpajoissa erityisen huolissaan. Digitalisaation vaihtoehdottomuus esimerkiksi peruspalveluiden järjestämisessä sivuuttaa henkilöt, joilla ei ole laitteita ja yhteyksiä, taloudellisia resursseja näiden hankkimiseen, mahdollisuutta käyttää virtu-pisteitä tai riittävää taitotietoa digitaaliseen asiointiin. Samalla digitalisoituva palvelutarjonta asettaa uusia vaatimuksia sähkö- ja televiestintäverkkojen suorituskyvylle etenkin harvaan asutuilla alueilla.

Työpajoissa kerrottiin, että Enontekiöllä ollaan riippuvaisia nettipalveluista. Hyviä palveluita oli saatavilla ja ne tuottivat käyttäjilleen kustannussäästöjä. Niistä luopuminen tuntuisi hankalalta, vaikka digitaalisten palveluiden käyttö oli tavallaan ”pakon sanelemaa, kun tässä ei ole mitään lähellä”. Kaikkia palveluita ei itse löytänyt tai palveluiden käyttöön ottamiseen meni aikaa. Osa palveluista oli hyväksytty vasta, kun joku oli kädestä pitäen opastanut niiden käytössä. Työpajoissa todettiin, että jokin eettinen vastuu pitäisi olla tahoilla, jotka pakottivat ottamaan digitaalisia järjestelmiä käyttöön. Vastuuvaatimus liittyi paitsi helppokäyttöisyyteen myös tietojen keräämiseen, turvassa pitämiseen ja jatkokäyttöön. Esimerkiksi liian pitkälle menevää asiakasprofilointia ja siitä seuraavaa mainontaa karsastettiin. Jatkuvasti vastaan tuli kuitenkin palveluita, joita ei voinut käyttää, ellei hyväksynyt käyttöehtoja. Näissä tilanteissa valintaa tietojen käyttöön antamisesta tai antamatta jättämisestä ei pidetty todellisena valintana. (Myös Saariketo 2015, 131–132; Sirkkunen 2016; ks. van Dijck 2013, 170–171.) Digitalisaation myötä yksilön koettiin menettäneen hallinnan siitä, mitä tietoja hänestä kerättiin. Vaikka digitaaliset palvelut, ja etenkin sosiaalinen media, tarjoavat uusia mahdollisuuksia asioiden hoitamiseen ja vuorovaikutukseen, yksilöt kokevat, ettei kehitys ole heidän hallinnassaan (van Dijck 2013, 158–159). Hallinnan menettäminen lisää turvattomuuden tunnetta.

Palvelukokemukseen vaikuttaa resurssien keskittämisen aiheuttama paikallistuntemuksen katoaminen. Työpajoissa pahoiteltiin, ettei asioita hoitaakseen pystynyt soittamaan lähimpään palvelupisteeseen, vaan ainoastaan valtakunnalliseen numeroon: soittaessa jonot olivat pitkiä ja palveluvalikot monimutkaisia, kännykällä ei välttämättä saanut numerovalikkoa esiin etkä tiennyt, kenen kanssa puhuit tai missä tämä henkilö oli. Tsäteissä vastattiin huonosti tai vastaajana oli botti. Asiakaspalvelijat eivät aina tienneet, missä Enontekiö oli, eivät tunnistaneet paikallisia tiennimiä, joista osa on saamenkielisiä, tai eivät huomioineet, että esimerkiksi KELA-taksin saapuminen useamman sadan kilometrin päästä vei aikaa enemmän kuin varttitunnin. Hämmennystä aiheutti myös viranomaisviestintä suomi.fi-palveluportaalissa, jonka sähköpostia henkilö ei ollut ottanut käyttöön ennen kuin postitse tuli muistutus vastaamattomasta viestistä. Henkilökohtainen asiointi onnistui parhai-

ten kiertämällä valtakunnalliset järjestelmät ja laittamalla sähköpostia esimerkiksi suoraan paikallispankin johtajalle. Joillakin viranomaisilla oli vielä määräpäivinä palvelupiste Hetassa. Palvelujen kasvottomuus, asioinnin monimutkaisuus, epävarmuus oikean tiedon saamisesta, selittämisen tarve ja yllätykset heikentävät nekin ennakoinnin mahdollisuutta arkipäivässä ja lisäävät turvattomuutta.

Riittävien digitaitojen saavuttaminen on yksi suurimmista digitalisaatioon liittyvistä haasteista. Työpajoissa kerrotun mukaan itsepalvelukulttuurin kehittyminen vähensi inhimillisyyttä kohtaamisissa ja jätti taitamattomat ulkopuolelle. Eri ikäryhmien netin käyttöön tottumisen tai tottumattomuuden lisäksi yksilöiden asenteiden nähtiin tuottavan eroja osaamisessa. Osa työpajaosallistujista sanoi opetelleensa riittävät taidot itse tai kysyneensä lisäneuvoja muilta. Osa totesi, ettei heillä ollut aikaa tai kiinnostusta lähteä digitaalisuuteen mukaan kuin välttämättömissä määrin. Myös epävarmuus omista taidoista saattoi estää mahdollisuuksien hyödyntämisen. Neuvonta ja ohjaus nähtiin tärkeiksi, mutta järjestämisvastuuta koskevien kysymysten todettiin olevan auki koko yhteiskunnassa. Väestöpohjaltaan pienissä kunnissa työntekijät olivat ”sekaosaajia”, mutta kukaan ei pystynyt auttamaan kaikessa digitaalisessa. Tilanne on ongelmallinen etenkin yksilöturvallisuudelle.

Digitaidot liittyvät tietoturvan, tietosuojan ja yksityisyyden teemaan. Enontekiöläiset seurasivat kyberturvallisuusuutisointia ja osa koki meneillään olevan kehityksen pelottavaksi, koska arkipäivän toimivuus oli ”verkon varassa”. Työpajoissa nousi esiin koko yhteiskuntaa koskevan kybertapahtuman mahdollisuus, esimerkiksi televiestinnän lamauttaminen tai ydinvoimalaan murtautuminen. Aktiivisesti pohditut uhkat liittyivät kuitenkin arkipäiväisiin tilanteisiin. Omalla käytöksellä uskottiin olevan vaikutusta tietoturvaan ja tietosuojaan. Osa kertoi varovansa, mille sivuille netissä menee ja jättävänsä turhat linkit avaamatta. Sosiaaliseen mediaan osa suhtautui varauksella, koska esimerkiksi alustojen levittämistä viruksista ja huijauksista oli uutisoitu. Myös kunnassa oli kokemusta sähköpostihuijausyrityksestä, joka oli kilpistynyt henkilökunnan tarkkaavaisuuteen. Huijausten ja tietojen kalastelemisen estäminen on keskeinen tietoturvallisuushaaste, johon liittyvän taitotiedon ylläpitämiseksi ei ole täydellistä keinoa (esim. Junger, Montoya ja Overink 2017). Viranomaiset, media ja tietoturvayritykset julkaisevat ratkaisuksi listauksia asioista, joista huolehtimalla omaa ja muiden digitaalista turvallisuutta voi parantaa. Lainsäädännössä yksilöä vastuutetaan turvallisuudesta tapauskohtaisella arvioinnilla siitä, mitä yksilön olisi pitänyt tietää ja osata tai mitä hänen olisi perustellusti voinut odottaa tietävän ja osaavan. Missään ei kuitenkaan ole yleispätevästi määritelty vaadittavien digitaitojen tasoa. (Päläs ja Salminen 2019.) Vastuuttaminen on jossain määrin onnistunut, koska ajatus oman toiminnan vaikutuksesta digitaaliseen turvallisuuteen nousi keskusteluissa esiin.

Eri palveluihin tarvittavien salasanojen määrä mainittiin työpajoissa haasteeksi, sillä kaikkien muistamiseen tarvittaisiin muistikirja, joka varastettaisiin tai unohtuisi johonkin. Tietosuoja nousi esiin etenkin neuvonnan ja ohjauksen teeman yhteydessä. Kaikki eivät halua kertoa yksityisasioistaan neuvojalle ja jatkuva kyseleminen koettiin epämiellyttäväksi. Yksityisyyteen suhtauduttiin vaihtelevasti: Osa oli valmis luopumaan siitä, jotta viranomaisille saataisiin riittävät valtuudet valvoa ja puuttua rikolliseen toimintaan. Osa oli vahvasti rajoittamatonta valvontaa vastaan. Tutkimuksen mukaan suhtautuminen viranomaisvalvontaan onkin kaksijakoista, vaikka nettikäyttäjät ovat huolissaan yksityisyydes-

tään (Sirkkunen 2016, 118, 128–129). Keskusteluissa esitettiin epäilyksiä viranomaisten digitaalisten palveluiden tietoturvaa ja tietosuojaa kohtaan. Todettiin, että olisi pystyttävä täydellisesti luottamaan siihen, että viranomaisilla tiedot olivat ”siellä missä pitääkin ja turvallisesti tallessa”. Myös kunnan koettiin olevan tästä omalta osaltaan vastuussa. Seppäsen ja Väliverrosen (2012) mukaan kyky luottaa instituutioihin on olennainen osa turvallisuuden tunnetta.

Sosiaalisen median negatiiviset piirteet nostettiin työpajoissa useasti esiin. Ne liittyivät pääosin vihapuheeseen ja perättömiin kirjoituksiin, tietoturvaan, tietosuojaan ja yksityisyyteen sekä valvontaan. Ongelmien huomautettiin olevan siellä, mistä valvonta puuttui, ja alustoille ehdotettiin kellonaikaa, minkä jälkeen niille ei voisi kirjoittaa. Sosiaalisen median nähtiin edesauttavan häiriköintiä (minkä tutkimus on vahvistanut: esim. Stiff 2019) ja mahdollistavan paikallisiin asioihin puuttumisen etäisyyksien takaa, mikä oli kohdistunut etenkin saamelais- ja maahanmuuttajakysymyksiin. Todettiin, että haukkumiseen ja valehteluun ei puututtu riittävästi ja että sitä tapahtui sosiaalisen median ulkopuolellakin. Omien tai kylän oikeuksien puolustaminen koettiin hankalaksi, koska se johti helposti ilkeilyn tai vihapuheen kohteeksi joutumiseen. Väärää tietoa kerrottiin laitettavan liikkeelle ja asioita vääristeltävän tarkoituksellisesti, lievimmillään harkitsemattoman ”somekirjoittelun” katsottiin johtavan väärinymmärryksiin. Kasvottomuuden taakse sanottiin netissä olevan helppo piiloutua ja jonakin toisena esiintymisen liittyvän myös brändäämiseen, kun ”voit valita minkälainen olet” (myös Montgomery 2015, 774; Vainikka ja Harju 2019, 102). Vaaraksi nähtiin oman identiteetin kadottaminen.

Sosiaalisen median negatiiviset piirteet olivat johtaneet siihen, että osa keskustelijoista pysytteli alustoilta pois tai käytti niitä rajallisesti esimerkiksi tiedon hankkimiseen. Sen sijaan pikaviestintäpalveluita käytettiin aktiivisesti kuulumisten vaihtamiseen ja yhteyden pitämiseen kaukanakin asuviin sukulaisiin ja tuttaviin. Tämän tutkimuksen teemoista sosiaalinen media ja pikaviestintäpalvelut selkeimmin jakavat kokemukset inhimillistä turvallisuutta parantaviin ja heikentäviin. Digitaalista turvallisuutta rakennetaan samoissa sosiaalisissa käytännöissä ja vuorovaikutuksessa kuin tieto- ja viestintäteknologiaa. Teknologia ei ole neutraalia, muttei myöskään yksiselitteisesti voimaannuttavaa tai turvattomuutta tuottavaa vaan molempia (van Dijck 2013, 18). Sosiaalisen median rakenne ja algoritmit muokkaavat inhimillistä vuorovaikutusta. Oletusasetukset heijastelevat alustan omistajien strategisia valintoja, jotka saattavat olla ristiriidassa alustan käyttäjien arvojen, tarpeiden ja toiveiden kanssa. Esimerkiksi sosiaalisessa vuorovaikutuksessa syntyvä metadata ja sen kaupallistaminen pitävät yllä keskustelua siitä, kuka datan omistaa – henkilöt, joista se on kerätty vai yritys, joka sen on kerännyt. Sosiaalisissa käytännöissä määrittyy myös se, millainen sosiaalisen median käyttö ja millainen tiedonkeruu on hyväksyttävää ja luottamusta ylläpitävää. Epäsuotavaksi normitettua toimintaa pyritään kitkemään muun muassa yksityisyyden/avoimuuden tai turvallisuuden nimissä, joiden määrittely on kuitenkin aikaan ja paikkaan sidoksissa. (Van Dijck 2013, 29–30, 34, 174.) Turvattomaksi koetusta vuorovaikutuksesta ihmiset pyrkivät mahdollisuuksiensa mukaan pois, ellei siitä saatavia hyötyjä arvioida haittoja suuremmiksi.

Viimeisinä työpajakeskusteluista nousseina inhimillisen turvallisuuden haasteina ovat ympäristönäkökohdat sekä koneiden ja laitteiden korjattavuus, jotka liittyvät toisiinsa. Digitalisaation ja ympäristöturvallisuuden suhde on monimutkainen. Työpajoissa kerrotun

mukaan digitalisaatio vähensi matkustamisen tarvetta ja päästöjä. Tietoteknisten laitteiden lyhyt elinkaari lisäsi elektroniikkajätettä, uusien satelliittien lähettäminen avaruuteen avaruusromun määrää ja laitteiden lisääntyminen laitesäteilyn vaikutuksia. Ympäristön kannalta kuluttamista pitäisi vähentää, mutta talouden kannalta lisätä, mikä kertoi järjestelmän epätasapainosta. Koneiden ja laitteiden digitaalisuus vähensi niiden korjattavuutta, mikä lisäsi kuluja ja matkustamistarvetta, kun esimerkiksi auto oli paikallisesti tehdyn korjauksen jälkeen ajettava satojen kilometrien päähän, jotta sen katsastuksesta läpi menemisen estävä merkkivalo saatiin nollattua. Netti helpotti varaosien etsimistä, kun taas ohjekirjojen digitoiminen teki niistä hyödyttömiä esimerkiksi sähkökatkon aikana, jolloin olisi tarvittu apua digitaalisen talotekniikan kanssa. Etäkorjattavuus nähtiin vielä hyödyntämättömäksi digitalisaation mahdollisuudeksi. Politiikkaohjelmissa digitalisaation ympäristövaikutukset arvioidaan yleensä positiivisiksi (saasteiden väheneminen), mutta enontekiöläisten kertoma nostaa esiin aiheen monimutkaisuuden (mm. sähkönkulutuksen lisääntyminen). Digitalisaation ja ympäristöturvallisuuden suhteesta tarvitaankin lisää tutkimusta. Digitalisaatioon liittyvät mahdollisuudet ja haasteet ovat läsnä rinnakkain, minkä vuoksi positiivista ja negatiivista turvallisuutta tulee tarkastella yhdessä. Normalisoituessaan mahdollisuuksia ja haasteita tuottavat tekijät vakiintuvat rakenteiksi, jotka edistävät tai estävät toivotunlaista digitaalista kehitystä, samalla muokaten käsityksiä siitä, mikä on toivotunlaista kehitystä (ks. van Dijck 2013, 19–20).

Toivotunlaista digitaalista kehitystä edistävät tekijät ja sen esteet

Työpajakeskustelujen perusteella toivotunlaista kehitystä edistävät toimivat ja helppokäyttöiset digitaaliset palvelut, paikalliset palvelut ja sovellukset, tietoturva, tietosuoja ja yksityisyys sekä yksilön ja yhteisön turvallisuutta lisäävä valvonta. Kehitystä taas vaikeuttavat pitkät etäisyydet ja paikallistuntemuksen puute, resurssien keskittäminen, sähkö- ja televiestintäverkkojen haavoittuvuudet ja näihin liittyen riippuvuus nettipalveluista, vaillinaiset digitaidot, itsepalvelukulttuuri ja puutteellinen neuvonta ja ohjaus, digitalisaation vaihtoehdottomuus ja varjopuolet kuten vihapuhe ja perättömät kirjoitukset. Lisäksi teknologian nopea kehitys asettaa haasteita yhteiskunnan digitalisaatiolle ja sen ohjaamiselle. Digitalisaation tavoiteltavuus nousikin yhdeksi keskustelluista teemoista. Enontekiön kunnassa haluttiin kannustaa digitaalisuuteen, koska se oli kustannustehokasta ja säästi henkilöstön aikaa vaativiin tehtäviin. Digitaalisuuteen siirtyminen toki vaati resursseja. Vaihtoehdoksi työpajakeskustelujen osallistujat visioivat Enontekiöstä ”digivapaata kuntaa”, jonka yhtenä matkailuvalttina olisivat sosiaalisesta mediasta irtautumisen retriitit. Todettiin, ettei kunnan ehkä halutakaan olevan digitalisaatiokunta. Digitalisaation tavoiteltavuuden teema tiivistää artikkelin aiemmissakin osioissa mainitut jännitteet digitaalisessa kehityksessä: kaikki eivät halua samoja asioita, mutta jotenkin yhteisestä suunnasta on päätettävä ja kaikkien osallisuudesta ja turvallisuudesta huolehdittava.

Työpajakeskusteluiden pääviesti oli, että digitalisaatiota pitäisi viedä inhimillisempään, hyvinvointia lisäävään suuntaan. Esimerkiksi videokuvan tuleminen osaksi netissä tapahtuvaa yhteydenpitoa oli lisännyt turvallisuuden tunnetta. Palveluista ei saisi tulla täysin kasvottomia, koneellisia ja automatisoituja tai valikoiden ja tsättibottien hoitamia, eikä ihmisiä saisi ohjata vain ”menemään nettiin ja katsomaan sieltä”. Itsepalvelukulttuurin kat-

sottiin johtaneen siihen, että vaikka asiakas täydensi tietoja järjestelmään, ei häntä tiedotettu asian käsittelyn vaiheista. Vastavuoroisuuden puuttuessa oli vaikea tietää, oliko tullut ymmärretyksi oikein ja voiko asioiden etenemiseen luottaa. Kysymys siitä, mihin digitaalisuudessa ylipäänsä voi luottaa nousi keskusteluun. Limnéllin ja kumppaneiden (2014, 40) mukaan digitaalisen toimintaympäristön voi ”arvioida turvalliseksi, kun sen toimivuuteen voi luottaa”, mihin enontekiöläisten kertoman mukaan on vielä matkaa. Työpajoissa digitalisaation todettiin myös eriarvoistavan muun muassa asuinpaikan, digitaitojen ja varallisuuden perusteella. Eriarvoisuuteen nähtiin kyettävän vaikuttamaan vain vaatimalla perusoikeuksien toteutumista (vrt. Brown ja Ainley 2009, 221–222).

Lainsäädännöllä ja lain toimeenpanolla katsottiinkin olevan vaikeuksia pysyä muutoksessa mukana. Lain ja poliisin ei uskottu pystyvän täysin vastaamaan digitaalisia keinoja käyttävään rikolliseen toimintaan. Tutkimus muun muassa Yhdysvalloista tulee samaan johtopäätökseen: Voimassa olevalla lainsäädännöllä ei pystytä kitkemään haitallisten sisältöjen leviämistä esimerkiksi sosiaalisessa mediassa eikä alan yrityksillä ole riittävää tahtoa rakentaa turvallisia alustoja. Koska valtaosa suosituimmista sosiaalisen median yrityksistä on yhdysvaltalaisia, on tällä merkitystä yksilöiden ja yhteisöjen hyvinvointiin globaalisti, vaikka paikallisella lainsäädännöllä onkin voitu jonkin verran lisätä digitaalista turvallisuutta. (Montgomery 2015, 778–779; Grygiel ja Brown 2019.) Työpajoissa osa keskustelijoista näki, että vahvemmalla viranomaisvalvonnalla voitaisiin vähentää väärinkäytöksiä. Osa painotti, että oli olennaista tietää, kuka tietoja keräsi ja valvontaa suoritti, mihin tietoja käytettiin ja miten niiden pohjalta toimittiin. Lainsäädäntö on henkilökohtaisen eettisen toiminnan, sosiaalisen paineen sekä tieto- ja viestintäteknologian alan yritysten ja muiden toimijoiden välisen sopimisen ohella keino, jolla raamitetaan digitaalista kehitystä ja sen suuntaa. Teema liittyy vielä käsittelemättä oleviin yksilön vaikutusmahdollisuuksiin ja eri toimijoiden rooleihin.

Yksilön vaikutusmahdollisuudet digitaaliseen kehitykseen ja eri toimijoiden roolit digitaalisen turvallisuuden tuottamisessa

Yksilön kyky vaikuttaa digitalisaatioon nähtiin työpajoissa heikoksi. Vaikutusmahdollisuudet rajoittuivat lähinnä omaan ja läheisten, etenkin lasten, käyttäytymiseen ja palveluiden käyttöön ottamiseen tai käytämättä jättämiseen. Useimmista tuntui, että muutokset tulivat aina jostakin eikä itse voinut kuin sopeutua. Moni ei myöskään ollut ajatellut omaa tarvettaan tai haluaan vaikuttaa kehityksen suuntaan. Keskustelijat kokivat olevansa muutoksissa palveluntarjoajien, televiestintäyhteyksien ylläpitäjien ja yhteiskunnan päätösten kohteina. Päätöksiin pitäisi silti pystyä vaikuttamaan esimerkiksi ottamalla yhteyttä yhteiskunnallisiin päättäjiin. Enontekiöläisten kokemus tukee inhimillisen turvallisuuden näkökulman kritiikkiä siitä, että digitalisaatiossa ja siihen liittyvässä turvallisuusajattelussa yksilöt ja yhteisöt nähdään pääasiallisesti toiminnan kohteina – ei aktiivisina toimijoina, joiden tulisi olla mukana määrittelemässä kehitykseen liittyviä mahdollisuuksia ja uhkia ja päättämässä toimintatavoista.

Toimijoille yhteiskunnan eri tasoilla löydettiin keskusteluissa oma roolinsa digitaalisen turvallisuuden tuottamisessa. Yksilöiden oman eettisen toiminnan katsottiin olevan merkityksellistä. Jokaisella oli vastuu ylläpitää turvallisuutta: arvioida omaa käytöstään ja toimia

annettujen ohjeiden mukaan. Järjestöillä, varsinkin ihmisten parissa työtä tekevillä, oli vastuu tietoturvasta, tietosuojasta ja yksilöiden auttamisesta. Yrityksillä oli vastuu tuotteiden ja palveluiden helppokäyttöisyydestä sekä asiakaspalvelijoiden osaamisesta. Tietoturvasta ja tietosuojasta oli huolehdittava, eikä epäonnistumisia ja vastuuta virheistä voinut jättää asiakkaille. Myös palveluiden ostajilla oli sopimusvastuu palveluista ja niiden turvallisuudesta. Kunnan piti olla luotettava asukkailleen, hallintoalueiden vastata omista alueistaan ja toimialojen omista palveluistaan ja näiden turvallisuudesta. Asioidessaan minkä tahansa viranomaisen kanssa kansalaisen pitäisi pystyä luottamaan toimijaan täysin. Tietyt asiat työpajaosallistujien mukaan oli pakko hoitaa valtakunnallisesti tai jopa Euroopan unionissa. Vastuu oli ketjutettu kaikille tasoille ja monesta asiasta sovittu lakisääteisesti. Työpajaosallistujien jäsennys eri toimijoiden rooleista digitaalisen turvallisuuden tuottamisessa on esimerkiksi Suomen kokonaisturvallisuusjärjestelmän mukainen. Eri toimijoiden rooleja on kuitenkin vaikea täsmentää, sillä rajapinnoista ei ole selkeästi sovittu ja vastuunjako on tilannekohtaista (esim. Lehto ym. 2018).

Inhimillinen turvallisuus digitaalisena turvallisuutena

Inhimillisen turvallisuuden näkökulmasta digitaalinen turvallisuus sisältää ne digitalisaatioon liittyvät tekijät, jotka (1) parantavat tai ylläpitävät hyvinvointia ja/tai (2) heikentävät hyvinvointia tai estävät tai heikentävät hyvinvointia parantavien tekijöiden vaikutusta. Tekijät ja niiden vaikutukset voivat sijaita digitaalisessa tai fyysisessä toimintaympäristössä, sillä nämä ympäristöt sulautuvat vähitellen yhteen. Digitaalisessa turvallisuudessa suojattavina kohteina ovat yksilöt ja yhteisöt digitalisoituvassa arkipäivässään. Näkökulma on aika- ja paikkasidonnainen eikä turvallisuus liity pelkästään vaaratilanteisiin vaan on olennainen osa jatkuvaa inhimillisen hyvinvoinnin vahvistamista. Ihmiset tulisi nähdä turvallisuuden tuottajia, jotka osallistuvat päätöksentekoon hyödynnettävistä digitalisaation mahdollisuuksista, näihin liittyvistä uhkista ja turvatoimista – ei siis pelkästään turvatoimien kohteina. Kuten tästä artikkelista käy ilmi, arkipäivän jäsennys digitaalisesta turvallisuudesta on osin yhteneväinen, mutta osin myös poikkeaa niin teknisestä kuin strategisesta tieto- ja kyberturvallisuusmäärittelystä, mikä pitäisi huomioida yhteiskunnan kokonaisturvallisuuden järjestelyissä.

Digitaaliseen turvallisuuden tuottamisessa yksilöiden digitaidoilla on suuri rooli, mutta vastuunjakoa yhteiskunnan eri toimijoiden välillä on selkiytettävä, jotta vastuu jakautuu kohtuullisesti eikä eriarvoisuus enää lisäänny. Ketään ei voida pakottaa opettelemaan digitaitoja, mutta digitalisaatio etenee yksilöiden tahdosta riippumatta, synnyttää digitaalisia kuiluja ja nostaa digitaidottomien asiointikustannuksia, mikä vähentää luottamusta ja lisää turvattomuutta samaan aikaan, kun digitalisaatio avaa uusia mahdollisuuksia myös harvaan asutuilla alueilla. Digitaalisen turvallisuuden tavoitteena ei ole kaiken mahdollisen turvallistaminen vaan niiden digitalisaatioon liittyvien ongelmien esiin tuominen, jotka vaativat ratkaisua, kuten eriarvoistumisen pysäyttäminen ja perusoikeuksista huolehtiminen. Tavoitteena on yksilöiden ja yhteisöjen hyvinvointi, mikä edellyttää inhimillisen turvallisuuden tilaa, jossa digitalisaation mahdollisuudet ja uhkat ovat tasapainossa.

Liite 1

Enontekiön työpajakeskusteluista nousevat teemat (suluissa rakenteelliset teemat, joiden alle työpajakeskusteluista nousevien teemojen sisältöjä on sijoiteltu analyysissa).

VI	Puhelimen keskeisyys (I, IIa)
VII	Sähkö- ja televiestintäverkot (I, IIb, III)
VIII	Etäisyydet ja paikallistuntemus (I, IIa, IIb, III)
IX	Ennakoiminen (IIa)
X	Netin kautta tilaaminen (I, IIa, IIb)
XI	Paikalliset palvelut ja sovellukset (IIa, IIb, III)
XII	Avunsaanti (I, IIa, IIb)
XIII	Terveys ja hyvinvointi (I, IIa, III, V)
XIV	Asiointi (I, IIa, IIb, III)
XV	Pelaaminen (I, IIa)
XVI	Kulttuuri- ja sivistystoimi, harrastukset (I, IIa)
XVII	Opiskelu ja tiedonsaanti (I, IIa)
XVIII	Työn muutos (I, IIa)
XIX	Ympäristönäkökohdat (I, IIa, IIb)
XX	Riippuvuus nettipalveluista (I, IIa, IIb, III, V)
XXI	Digitalisaation tavoiteltavuus (IIb, III)
XXII	Digitalisaation vaihtoehdottomuus (I, IIa, IIb, III)
XXIII	Koneiden ja laitteiden korjattavuus (IIb)
XXIV	Digitaidot (I, IIa, IIb, III, V)
XXV	Itsepalvelukulttuuri, neuvonta ja ohjaus (I, IIa, IIb, III, V)
XXVI	Sosiaalinen media ja pikaviestintäpalvelut (I, IIa, IIb, V)
XXVII	Tietoturva, tietosuoja ja yksityisyys (I, IIa, IIb, III, V)
XXVIII	Vihapuhe ja perättömät kirjoitukset (IIa, IIb, III)
XXIX	Valvonta (IIa, IIb, III)
XXX	Lainsäädäntö ja lain toimeenpano (I, III, V)
XXXI	Yhdenvertaisuus ja vastavuoroisuus (I, IIb, III)
XXXII	Resurssien keskittäminen (IIa, IIb, III)
XXXIII	Koko yhteiskuntaa koskevan kybertapahtuman mahdollisuus (IIb)
XXXIV	Eri ikäryhmät (I, IIa, IIb)
XXXV	Inhimillisyys ja luottamus (I, IIa, IIb, III, V)
XXXVI	Teknologian nopea kehitys (I, III)

Viitteet

1 Enontekiön kunnan www-sivut: https://enontekio.fi/, erityisesti ”Tietoa Enontekiöstä”. Vuoden 2015 luvut sivujen mukaan: alkutuotanto 9,9 %, jalostus 10,7 %, palvelut 75,8 % ja muut 3,6 %. Ilmasto-opas.fi-sivusto, erityisesti ”Pohjois-Lappi – Jäämeren vaikutuksessa” https://ilmasto-opas.fi/fi/ilmastonmuutos/suomenmuuttuva-ilmasto/-/artikkeli/1a8caec6-3b73-4dc8-a957-febe69188aeo/pohjois-lappi-jaameren-vaikutuksessa.html.

2 Tunturi-Lapin muodostavat Enontekiön, Muonion, Kittilän ja Kolarin kunnat.

3 Lapin ELY-keskus. 2018. ELY-keskuksen myöntämä rahoitus Lapin maakuntaan 1.1.–30.6.2018. Luettu 10.3.2020. https://www.ely-keskus.fi/documents/10191/429489/Rahoituslistaus+tammikes%C3%A4kuu+2018/of1fcof6-7452-48e5-a414-3068e3391ba9.

4 YLE. 18.1.2019. Holopainen, Hanna. Käsivarresta vedettiin valokaapeli Norjaan – nopeat yhteydet voivat houkutella datakeskuksia. Luettu 3.3.2019. https://yle.fi/uutiset/3-10601259.

5 Liikenne- ja viestintävirasto. 2020. Kiinteän verkon laajakaistasaatavuus. Luettu 6.3.2021. https://www.traficom.fi/fi/kiintean-verkon-laajakaistasaatavuus.

6 2 Mbit/s 54,6 % kotitalouksista, 10 Mbit/s 38 % kotitalouksista, 30 Mbit/s 17,7 % kotitalouksista ja 100 Mbit/s 11,3 % kotitalouksista.

7 Kuluttajilla ja yrityksillä on oikeus saada tietyt kohtuuhintaiset ja toimivat viestinnän peruspalvelut eli yleispalvelut (kiinteä tai langaton puhelinliittymä, 2 Mbit/s internetliittymä, kuulo- ja puhevammaisten tekstiviesti- ja internetpalvelu sekä kattava yhteystietopalvelu) kotiinsa tai yrityksen toimipisteeseen. Liikenne- ja viestintävirasto nimeää operaattorin tarjoamaan yleispalveluja niillä alueilla, joilla ei muuten olisi riittävästi kaupallista tarjontaa. Liikenne- ja viestintäviraston www-sivut: https://www.traficom.fi/fi/viestinta/laajakaista-ja-puhelin/oikeutesi-viestinnan-peruspalveluihin.

8 Liikenne- ja viestintäviraston MONITORi-palvelu: https://eservices.traficom.fi/monitori/area.

9 YLE. 30.8.2017. Torikka, Raimo. Kylät talkoilevat valokuituverkkoja teleoperaattoreiden hyväksi. Luettu 4.3.2019. https://yle.fi/uutiset/3-9803954.

10 Tapaustutkimus on osa Enablement besides Constraints: Human Security and a Cyber Multi-disciplinary Framework in the European High North (ECoHuCy) -projektia, jonka rahoittivat NordForsk ja Economic and Social Research Council (ESRC) vuosina 2017–2019. Kiitokset Enontekiön työpajoihin osallistuneille ja Tapio Nykäselle, Jenna Päläkselle ja Pertti Salmiselle kommenteista kirjoitusprosessin aikana.

11 Lapin liitto 2013; Enontekiön kunta (2018). Met tehemä yhessä -strategia 2025. Luettu 2.3.2019. https://enontekio.fi/kunta-ja-hallinto/talous-ja-strategia/talous-ja-strategia/.

12 Valtiovarainministeriö. 2020. Digitalisaation edistämisen ohjelma 2020–2023. Toimintasuunnitelma 2020. Luettu 28.1.2021. https://vm.fi/documents/10623/1464506/Digitalisaation+edist%C3%A4misen+ohjelman+toimintasuunnitelma/5cd124e3-ec59-2fcb-79e0-a501f7ec404c/Digitalisaation+edist%C3%A4misen+ohjelman+toimintasuunnitelma.pdf.

13 Valtionvarainministeriön www-sivut, erityisesti ”Digitalisaatio”: https://vm.fi/digitalisaatio.

14 Kohti esteetöntä viestintää -toimenpideohjelma oli ensimmäinen politiikkaohjelma, jossa selvitettiin ”millaisia toimenpiteitä viestintäpalveluiden esteettömyyden takaaminen nyt ja tulevaisuudessa edellyttää” sekä kerättiin ”tietoa viestintäpalveluiden esteettömyyteen […] liittyvistä ongelmista” (Liikenne- ja viestintäministeriö 2005, 5). Luettu 18.7.2016. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/77838/OS1_2005.pdf.

15 Esimerkiksi YK:n päämajassa 2.–4.12.2019 pidetyssä konsultoivassa dialogissa – Informal intersessional consultative meeting of the OEWG (Open-ended working group on developments in the field of information and telecommunications in the context of international security) with industry, non-governmental organizations and academia.

16 OECD erottaa www-sivuillaan käsitteet kyberturvallisuus ja digitaalinen turvallisuus. Kyberturvallisuus yhdistää neljä tulokulmaa: taloudellisen ja sosiaalisen, teknisen, lain täytäntöönpanon sekä kansallisen ja kansainvälisen turvallisuuden. Digitaalinen turvallisuus viittaa näistä taloudelliseen ja sosiaaliseen koskien yrityksiä, julkishallintoa, organisaatioita ja yksilöitä. Toimijat suojaavat turvallisuuttaan, omaisuuttaan, mainettaan, käytössä olevia mahdollisuuksiaan sekä toimintojensa jatkuvuutta häiriöiltä, jotka voivat vaikuttaa datan, verkkojen, ohjelmistojen ja laitteiden saatavuuteen, eheyteen ja/tai luotettavuuteen. https://www.oecd.org/internet/global-forum-digital-security/about/.

17 Keskustelutilaisuudet, Hetassa tiistaina 20.11.2018 ja Kilpisjärvellä torstaina 22.11.2018, järjestettiin yhteistyössä Enontekiön kunnan kanssa. Tilaisuudet alkoivat työpäivän jälkeen viideltä ja osallistujia oli pyydetty varaamaan pari, kolme tuntia aikaa. Tilaisuuksista tiedotettiin järjestävän tutkimusinstituutin viestintäkanavien (internetsivusto sekä sosiaalinen media) ohella Facebookiin luoduilla tapahtumilla sekä pyytämällä ihmisiä välittämään tietoa eteenpäin. Enontekiön kunta tiedotti keskusteluilloista omilla viestintäkanavillaan. Hetan keskeisimmälle paikalle, ruokakaupan ilmoitustaululle, vietiin tapahtumajuliste. Viikkoa ennen tapahtumia paikallislehti Enontekiön Sanomat julkaisi henkilöhaastattelun keskusteluja vetävästä tutkijasta, minkä yhteydessä esitettiin avoin kutsu työpajoihin.

18 Työpajoissa huomautettiin, että lapset ja nuoret tulisi saada tutkimukseen mukaan, sillä heidän kokemuksensa digitalisesta turvallisuudesta on erilainen. Enontekiön työpajoihin osallistujat olivat ikähaarukassa 30–80 vuotta. Pääosa heistä hyödynsi tieto- ja viestintäteknologiaa päivittäin eri tarkoituksiin.

19 Tutkimusasetelmasta johtuvat teemat, joilla on suoria ja epäsuoria vaikutuksia tutkimusaineistoon (Guest, MacQueen ja Namey 2012, 50).

20 Tutkimusasetelman mukaisessa keskustelussa havaitut tai keskustellut teemat, jotka nousevat vuorovaikutuksesta (Guest, MacQueen ja Namey 2012, 50).

21 Ks. Timo-Huhtala, Maria. 2018. Porokello - porovaroittaminen liikenteessä älyteknologian avulla. Loppuraportti 2016–2017. Lapin elinkeino-, liikenne- ja ympäristökeskus. Raportteja 4/2018. Luettu 7.4.2020. https://www.doria.fi/bitstream/handle/10024/149593/Raportteja_4_2018_Porokello.pdf.

22 ”Poron korviin kiinnitettäviä pilttoja käytetään [korvamerkin] lisämerkkeinä esimerkiksi ostettaessa elävinä jo aiemman omistajan merkkiin merkittyjä poroja. Pilttaa tarvitaan myös osoittamaan poro rekisteröidyksi kilpa- tai matkailuporoksi.” Paliskuntien yhdistyksen www-sivut: https://paliskunnat.fi/poro/, erityisesti ”Menetelmiä” ja ”Piltta”.

23 Toimiva kotihoito Lappiin -hanke oli Lapin maakunnan alueellinen hanke (1.10.2016–31.12.2018), jossa pyrittiin luomaan palvelujärjestelmä, jossa iäkkäät saavat pääosan tarvitsemistaan palveluista kotiin tai kotoa käsin. Hankkeessa mm. tuotettiin tietoa teknologia-avusteisten palvelujen haasteista ja hyödyistä kotona asuville ikäihmisille.

24 Virtu.fi on lappilaisten sähköisten sosiaali- ja terveyspalveluiden digitaalinen alusta. Enontekiöllä asiakaspisteitä on Hetassa, Karesuvannossa ja Kilpisjärvellä.

25 Kuitua pohjoiseen -hankkeessa (1.9.2015–31.8.2018) ja Kuitu kylässä -hankkeessa (1.6.2018–1.6.2020) pyrittiin edistämään ja tukemaan kyläverkkojen rakentamista ja lisäämään digitaalisuuteen liittyvää osaamista Lapissa.

Kirjallisuus

Anwar, Mohd, Wu He, Ivan Ash, Xiaohong Yuan, Ling Lija Li Xu. 2017. “Gender difference and employees’ cybersecurity behaviors.” *Computers in Human Behavior* 69: 437–443. https://doi.org/10.1016/j.chb.2016.12.040.

Brennen, Scott ja Daniel Kreiss. 2014. Digitization and Digitalization. Culture Digitally -ryhmäblogi. Luettu 3.3.2019. http://culturedigitally.org/2014/09/digitalization-and-digitization/.

Brotby, Krag. 2009. *Information Security Governance. A Practical Development and Implementation Approach.* Hoboken (NJ): John Wiley & Sons.

Brown, Chris ja Kirsten Ainley. 2009 [1997]. *Understanding International Relations.* Basingstoke: Palgrave Macmillan.

Buzan, Barry ja Lene Hansen. 2009. *The Evolution of International Security Studies.* Cambridge: Cambridge University Press.

Carr, Madeline. 2016. *US Power and the Internet in International Relation. The Irony of the Information Age.* New York (NY): Palgrave Macmillan.

Deibert, Ronald J. 2018. “Toward a Human-Centric Approach to Cybersecurity.” *Ethics and International Affairs* 32 (4): 411–424. https://doi.org/10.1017/S0892679418000618.

van Dijck, José. 2013. *The Culture of Connectivity. A Critical History of Social Media*. New York (NY): Oxford University Press.

Dunn Cavelty, Myriam. 2014. “Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities.” *Science and Engineering Ethics* 20 (2): 701–715. https://doi.org/10.1007/s11948-014-9551-y.

Fierke, Karin M. 2015 [2007]. *Critical Approaches to International Security.* Cambridge: Polity Press.

Gibson, William J. ja Andrew Brown. 2009. *Working with Qualitative Data.* London: SAGE.

Gomm, Roger. 2008 [2004]. *Social Research Methodology. A Critical Introduction.* New York (NY): Palgrave Macmillan.

Guest, Greg, Kathleen M. MacQueen ja Emily E. Namey. 2012. *Applied Thematic Analysis.* Thousand Oaks (CA): SAGE.

Grygiel, Jennifer ja Nina Brown. 2019. “Are social media companies motivated to be good corporate citizens? Examination of the connection between corporate social responsibility and social media safety.” *Telecommunications Policy* 43 (5): 445–460. https://doi.org/10.1016/j.telpol.2018.12.003.

Hampson, Fen Osler. 2008. “Human Security.” Teoksessa *Security Studies. An Introduction*, toimittanut Williams, Paul D., 229–243. Abingdon: Routledge.

Hennink, Monique, Inge Hutter ja Ajay Bailey. 2011. *Qualitative Research Methods*. London: SAGE.

Hoogesen Gjørv, Gunhild. 2012. “Security by any other name: negative security, positive security, and a multi-actor security approach.” *Review of International Studies* 38 (4): 835–859. https://doi.org/10.1017/S0260210511000751.

Hoogesen Gjørv, Gunhild. 2017 [2010]. “Human Security: Lessons Learned from Afghanistan.” Teoksessa *Routledge Handbook of Security Studies*, toimittaneet Dunn Cavelty, Myriam ja Thierry Balzacq, 106–116. London: Routledge.

Hui, Yuk. 2016. *The Question Concerning Technology in China. An Essay in Cosmotechnics.* Falmouth: Urbanomic Media.

Jansson, Saara ja Tanja Sihvonen. 2018. "Kyberturvallisuus valtiollisena toimintaympäristönä ja siihen kohdistuvat uhkat." *Media & viestintä* 41 (1): 1–28. https://doi.org/10.23983/mv.69950.

Junger, Marianne, Lorena Montoya ja F.-J. Overink. 2017. "Priming and warnings are not effective to prevent social engineering attacks." *Computers in Human Behavior* 66: 75–87. https://doi.org/10.1016/j.chb.2016.09.012.

Kerr, Pauline. 2007. "Human Security." Teoksessa *Contemporary Security Studies*, toimittanut Collins, Alan, 91–108. Oxford: Oxford University Press.

Kilpeläinen, Arja ja Yrjö Nikunlassi, toim. 2006. Kylät muutoksessa. Hankkeet kylien hyvinvoinnin edistäjinä? Pohjois-Suomen sosiaalialan osaamiskeskuksen julkaisusarja 23. Oulu: Pohjois-Suomen sosiaalialan osaamiskeskus. Luettu 24.2.2020. https://www.sosiaalikollega.fi/poske/julkaisut/julkaisusarja/Julkaisu_23.

Kilpeläinen, Arja. 2016. *Teknologiavälitteisyys kyläläisten arjessa. Tutkimus ikääntyvien sivukylien teknologiavälitteisyydestä ja sen rajapinnoista maaseutusosiaalityöhön.* Väitöskirjatutkimus. Acta Universitatis Lapponiensis 316. Rovaniemi: Lapin yliopisto.

Kramer, Franklin C., Stuart H. Starr ja Larry K. Wentz, toim. 2009. *Cyberpower and National Security.* Dulles (VA): National Defense University and Potomac Books.

Lapin liitto. 2007. Lapin tietoyhteiskuntastrategia 2007–2010. Kilpailukyky – arjen tietoyhteiskunta – osallisuuden lisääminen. Luettu 3.3.2019. http://www.lappi.fi/lapinliitto/c/document_library/get_file?folderId=22575&name=DLFE-1086.pdf.

Lapin liitto. 2013. Lapin digiohjelma 2020. Luettu 3.3.2019. http://www.lappi.fi/lapinliitto/c/document_library/get_file?folderId=1457612&name=DLFE-21300.pdf.

Lapin liitto. 2016. Työn muutos ja digitalisaatio eri toimialoilla Lapissa. Luettu 3.3.2019. http://www.lappi.fi/c/document_library/get_file?folderId=683161&name=DLFE-30605.pdf.

Latham, Robert ja Saskia Sassen, toim. 2005. *Digital Formations: IT and New Architectures in the Global Realm.* Princeton (NJ): Princeton University Press.

Lehto, Martti, Jarno Limnéll, Tuomas Kokkomäki, Jouni Pöyhönen ja Mirva Salminen. 2018. Kyberturvallisuuden strateginen johtaminen Suomessa. Valtioneuvoston selvitys- ja tutkimussarjan julkaisuja 28/2018. Helsinki: Valtioneuvoston kanslia. Luettu 18.5.2018. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160717/28-2018-Kyberturvallisuuden%20strateginen%20johtaminen.pdf.

Lewis, Ted G. 2015 [2006]. *Critical Infrastructure Protection in Homeland Security. Defending a Networked Nation.* Hoboken (NJ): John Wiley & Sons.

Lilius, Reijo, toim. 1997. Suomi tietoyhteiskunnaksi - kansallisten linjausten arviointi. Sitra 159. Luettu 19.7.2016. https://media.sitra.fi/2017/02/27173357/sitra159-2.pdf.

Limnéll, Jarno, Klaus Majewski ja Mirva Salminen. 2014. *Kyberturvallisuus.* Jyväskylä: Docendo.

Martin, Mary ja Taylor Owen. 2010. "The Second Generation of Human Security. Lessons from the UN and EU experience." *International Affairs* 86 (1): 211–224. https://doi.org/10.1111/j.1468-2346.2010.00876.x.

Montgomery, Kathryn C. 2015. "Youth and surveillance in the Facebook era: Policy interventions and social implications." *Telecommunications Policy* 39 (9): 771–786. https://doi.org/10.1016/j.telpol.2014.12.006.

Pare, Daniel. 2005. "The Digital Divide: Why the 'The' is Misleading?" Teoksessa *Human Rights in the Digital Age*, toimittaneet Klang, Mathias ja Andrew Murray, 85–97. London: GlassHouse Press.

Päläs, Jenna ja Mirva Salminen. 2019. "Alustan asiakkaan vastuusta ja vastuuttamisesta yksilöturvallisuuden tuottamisessa – sopimusoikeudellinen näkökulma kyberturvallisuuteen jakamistaloudessa." Teoksessa *Jakamistalousjuridiikan käsikirja*, toimittaneet Päläs, Jenna ja Kalle Määttä, 319–380. Helsinki: Alma Talent.

Raisio, Harri, Alisa Puustinen, Mika Hyytiäinen ja Tarja Wiikinkoski. 2017. Kansan pulssilla. Tarkastelussa deliberatiiviset turvallisuuskahvilat. Vaasan yliopiston raportteja 1. Vaasa: Vaasan yliopisto. Luettu 11.4.2019. https://www.univaasa.fi/materiaali/pdf/isbn_978-952-476-728-6.pdf.

Renaud, Karen ja Stephen Flowerday. 2017. "Contemplating human-centred security & privacy research: Suggesting future directions." *Journal of Information Security and Applications* 34 (1): 76–81. https://doi.org/10.1016/j.jisa.2017.05.006.

Rätti, Osmo ja Henri Wallén. 2017. Porotalouden digitalisoituminen. Loppuraportti. Lapin yliopiston Arktinen keskus & Saamelaisalueen koulutuskeskus.

Saariketo, Minna. 2015. "Neuvotteluja sosiaalisen median arkkitehtuurisesta vallasta. Käyttäjien ja ei-käyttäjien suhtautuminen Facebookiin teknologiavälitteisenä tilana." *Media & viestintä* 38 (3): 128–146. https://doi.org/10.23983/mv.62084.

Salminen, Mirva. 2018. "Digital Security in the Barents Region." Teoksessa *Society, Environment and Human Security in the Arctic Barents Region*, toimittaneet Hossain, Kamrul ja Dorothée Cambou, 187–204. Abingdon: Routledge.

Salminen, Mirva. 2019. "Refocusing and Redefining Cybersecurity: Individual Security in the Digitalising European High North." *The Yearbook of Polar Law* 10. Leiden: Brill, 321–356. https://doi.org/10.1163/22116427_010010015.

Salminen, Mirva ja Kamrul Hossain. 2018. "Digitalisation and human security dimensions in cybersecurity: an appraisal for the European High North." *Polar Record* 54 (2). https://doi.org/10.1017/S0032247418000268.

Schou, Jannick ja Morten Hjelholt. 2018. *Digitalization and Public Sector Transformations*. Palgrave Pivot. Cham: Palgrave Macmillan.

Seppänen, Janne ja Esa Väliverronen. 2012. *Mediayhteiskunta*. Tampere: Vastapaino.

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

Sirkkunen, Esa. 2016. "Yksityisyys valvonnan verkoissa." *Media & viestintä* 39 (2): 117–136. https://doi.org/10.23983/mv.61429.

Stiff, Chris. 2019. "The Dark Triad and Facebook surveillance: How Machiavellianism, psychopathy, but not narcissism predict using Facebook to spy on others." *Computers in Human Behavior* 94: 62–69. https://doi.org/10.1016/j.chb.2018.12.044.

Tadjbakhsh, Shahrbanou ja Anuradha Chenoy. 2009 [2007]. *Human Security: Concepts and Implications.* Abingdon: Routledge.

United Nations Development Programme (UNDP). 1994. Human Development Report. Luettu 18.3.2019. http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf.

United Nations Development Programme (UNDP). 1999. Human Development Report. Luettu 18.3.2019. http://hdr.undp.org/sites/default/files/reports/260/hdr_1999_en_nostats.pdf.

Vainikka, Eliisa ja Auli Harju. 2019. "Anonyymien keskustelupalstojen julkisuus Marginaaliin jääneiden vertaistukea ja yhteiskuntakritiikkiä." *Media & viestintä* 42 (2): 99–121. https://doi.org/10.23983/mv.83374.

Viinamäki, Leena, Ville Kivivirta, Arto Selkälä, Olli Voutilainen, Antti Syväjärvi ja Asko Suikkanen. 2017. Ajasta ja paikasta riippumatta. Digikansalaisuus ja palveluiden saavutettavuus maaseudulla -hankkeen loppuraportti. Lapin AMK:n julkaisuja. Sarja A. Referee-tutkimukset 1/2017. Luettu 1.3.2019. http://www.theseus.fi/handle/10024/137218.

Wagner, Ben, Matthias C. Kettemann ja Kilian Veith, toim. 2019. *Research Handbook on Human Rights and Digital Technology. Global Politics, Law and International Relations*. Cheltenham: Edward Elgar.

Webster, Frank. 2006 [1995]. *Theories of the Information Society*. Abingdon: Routledge.

Wheeler, Deborah L. 2013. "Does the Internet Empower? A Look at the Internet and Development." Teoksessa *The Handbook of Internet Studies*, toimittaneet Consalvo, Mia ja Charles Ess, 188–211. Chichester: Wiley-Blackwell.

Wolfers, Arnold. 1952. "'National Security' as an Ambiguous Symbol." *Political Science Quarterly* 67 (4): 481–502.

Yan, Zheng, Thomas Robertson, River Yanb, Sung Yong Parka, Samantha Bordoffa, Quan Chena, ja Ethan Sprissler. 2018. "Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?" *Computers in Human Behavior* 84: 375–382. https://doi.org/10.1016/j.chb.2018.02.019.

Zimmermann, Verena ja Karen Renaud. 2019. "Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset." *International Journal of Human-Computer Studies* 131: 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005.

Zojer, Gerald. 2019a. "The Interconnectedness of Digitalisation and Human Security in the European High North: Cybersecurity Conceptualised through the Human Security Lens." *The Yearbook of Polar Law X*, 297–320. https://doi.org/10.1163/22116427_010010014.

Zojer, Gerald. 2019b. "Free and open source software as a contribution to digital security in the Arctic." *Arctic Yearbook 2019*. Luettu 10.3.2020. https://arcticyearbook.com/images/yearbook/2019/Scholarly-Papers/10_AY2019_Zojer.pdf.