Tuomas Heikkinen

KYBERTURVALLISUUDEN YLEISTAJUISTAMINEN

Opinnäytetyö

Tekniikan ammattikorkeakoulututkinto

Kyberturvallisuuden koulutus

2023

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Insinööri (AMK)
Tekijä	Tuomas Heikkinen
Työn nimi	Kyberturvallisuuden yleistajuistaminen
Toimeksiantaja	Digi- ja väestötietovirasto
Vuosi	2023
Sivut	47 sivua, liitteitä 3 sivua
Työn ohjaajat	Kimmo Kääriäinen

TIIVISTELMÄ

Kyberturvallisuus koskettaa jokaista meistä, ja sen takia sen pitäisi olla myös ymmärrettävää jokaiselle meistä. Tämän takia ymmärrettävämpään kyberturvallisuusviestintään olisi syytä kiinnittää enemmän huomiota. Tässä tutkimuksessa vastataan tähän tarpeeseen. Tutkimuksessa selvitetään, miten kyberturvallisuutta yleistajuistetaan, eli miten siitä voidaan viestiä ymmärrettävämmin kansalaisille. Tutkimuksen toimeksiantajana toimii Digi- ja väestötietovirasto. Opinnäytetyön tavoite on herättää keskustelua ymmärrettävämmästä kyberturvallisuudesta ja sen tarpeesta.

Teoriaosassa tarkasteltiin ymmärrettävää viestintää ja aiempia kyberturvallisuuden ja tieteen yleistajuistamisen tutkimuksia. Lisäksi tutustuttiin siihen, miten kyberturvallisuus koskettaa jokaista kansalaista. Kyberturvallisuuden yleistajuistaminen tarkoittaa tässä tutkimuksessa sitä, että kyberturvallisuudesta viestitään ymmärrettävästi ja viestintä räätälöidään sen mukaan, kenelle puhutaan. Viestinnän tulee olla kohderyhmälähtöistä, ja kohderyhmän tulee kyetä ymmärtämään viesti riippumatta omista lähtökohdistaan.

Tutkimus toteutettiin laadullisena. Tutkimusaineisto kerättiin teemahaastatteluna, jossa haastateltiin 11 kyberturvallisuuden eritaustaista asiantuntijaa. Haastateltavat valittiin harkinnanvaraisesti siten, että jokaisen haastateltavan piti tuoda uusi ja erilainen näkökulma ilmiöön. Teemahaastattelut analysoitiin aineistolähtöisellä sisällönanalyysillä.

Tutkimustulosten perusteella kyberturvallisuuden yleistajuistamiselle nähtiin tarvetta. Yleistajuistamisessa kaikki lähtee siitä, että asiantuntija ymmärtää kohderyhmänsä ja räätälöi viestintänsä heille sopivaksi. Keskeistä on myös kyky poimia oleellinen asia ja viestiä se ymmärrettävästi. Esimerkit, vertauskuvien käyttö ja aiheen yhdistäminen arjessa jo läsnä oleviin asioihin edistävät ymmärrettävyyttä. Asiantuntija toimii ikään kuin tulkkina monimutkaisen kyberturvallisuuden ja kansalaisen välissä.

Tutkimus korostaa ymmärrettävän kyberturvallisuusviestinnän tarvetta. Tuloksissa voi olla ennalta-arvattavia asioita, etenkin viestinnän parissa jo toimiville. Tämä on hyväksyttävää, koska opinnäytetyön idea oli myös toimia perustutkimuksena aiheeseen. Opinnäytetyö tarjoaa ymmärrettävää tietoa viestinnästä, se siis osaltaan yleistajuistaa viestintää kyberturvallisuuden asiantuntijoille. Samalla tutkimuksen tarkoitus on kannustaa jatkotutkimusaiheiden tekemiseen, jotta kyberturvallisuudesta todella tehtäisi ymmärrettävää kaikille.

Asiasanat: kyberturvallisuus, yleistajuistaminen, teemahaastattelu, viestintä

Degree title	Bachelor of Engineering
Author	Tuomas Heikkinen
Thesis title	Popularisation of cybersecurity
Commissioned by	Digital and Population Data Services Agency
Time	2023
Pages	47 pages, 3 pages of appendices
Supervisor	Kimmo Kääriäinen

ABSTRACT

Cybersecurity affects each and every one of us, and that is why it should also be understandable to each and every one of us. Therefore, more attention should be given to making cybersecurity communication more understandable. This thesis addresses this need. It explores ways to popularise cybersecurity, that is, how to communicate it in a way that is more understandable to citizens. The objective of the thesis is to stimulate debate on the need for understandable cybersecurity.

The theoretical part of the study looked at understandable communication and previous research on cybersecurity and popularisation of science. It also explored how cybersecurity affects each of us. Popularisation of cybersecurity was defined, and in this study it means communicating about cybersecurity in a way that is understandable and tailored to the audience to whom it is addressed. The communication must be target group oriented and the target group must be able to understand the message regardless of their own starting point.

The research was qualitative. The data was collected through a focused interview with eleven experts with different backgrounds in cybersecurity. The interviewees were selected on a discretionary basis, so that each new interviewee had to bring a new and different perspective to the phenomenon. The focused interviews were analysed using a data-driven content analysis.

The results of the survey showed a need for popularisation of cybersecurity. Popularisation of cybersecurity is all about the expert understanding their target audience and tailoring their communication to suit them. The ability to pick up on what is important and communicate it in a way that is understandable is also key. The use of examples and metaphors and linking the topic to things that are already present in everyday life contributes to comprehensibility. The expert acts as an interpreter between the complex cybersecurity world and the citizen.

The study highlights the need for comprehensible cybersecurity communication. The results may be predictable, especially for those working in the field of communication. This is acceptable, as the idea of the thesis was also to serve as a foundation for the topic. The thesis provides understandable information on communication; thus, it contributes to the popularisation of communication for cybersecurity experts. At the same time, the purpose of the study is to encourage further research to make cybersecurity truly understandable to all.

Keywords: cybersecurity, popularisation, focused interview, communication

SISÄLLYS

1 JOHDANTO 5

2 TUTKIMUSSTRATEGIA 5

2.1 Tutkimusongelma 5

2.2 Tutkimusmenetelmät 6

2.3 Tutkimuksen vaiheet 8

2.4 Luotettavuusvarauma 11

3 TEOREETTINEN VIITEKEHYS 13

3.1 Ymmärrettävä viestintä 13

3.2 Tieteen yleistajuistaminen 15

3.3 Kyberturvallisuuden yleistajuistaminen 17

3.4 Näin kyberturvallisuuden viestintää on tutkittu 17

3.5 Kyberturvallisuus on jokaisen asia 18

3.6 Yhteenveto 20

4 TUTKIMUKSEN TEKEMINEN 21

5 TUTKIMUSTULOKSET 23

5.1 Kyberturvallisuudesta ymmärrettävämpää 23

5.2 Kyberturvallisuudesta kiinnostavampaa 27

5.3 Kyberturvallisuuden ymmärtämisen vastuu 30

5.4 Kyberturvallisuuden yleistajuistamisen tarve 32

5.5 Yhteenveto 36

6 JOHTOPÄÄTÖKSET 38

7 POHDINTA 41

LÄHTEET 45

LIITTEET

Liite 1. Teemahaastattelun kysymysrunko

Liite 2. Teemahaastattelun haastateltavien kuvaukset

1 JOHDANTO

Sillä on merkitystä, millä tavalla kyberturvallisuudesta viestitään. Tämä tutkimus haluaa tuoda tämän vahvemmin kyberturvallisuusalan keskusteluun mukaan. Tutkimuksessa tutkitaan, mitä kyberturvallisuuden yleistajuistaminen tarkoittaa ja miten yleistajuistamista voi tehdä – eli miten kyberturvallisuudesta voidaan viestiä ymmärrettävämmin kansalaisille.

Kyberturvallisuus on yhteiskunnan kannalta yhä ajankohtaisempi aihe ja kansalaisilla on yhä merkittävämpi rooli siinä. Suomen kyberturvallisuusstrategiassa sanotaan, että jokaisella kansalaisella tulisi olla riittävät valmiudet toimia turvallisesti digitaalisessa toimintaympäristössä (Turvallisuuskomitea 2019). Monissa yhteyksissä kyberturvallisuus nähdään myös kansalaistaitona (Limnéll ym. 2023; Lehto ym. 2017). Siksi on entistä tärkeämpää selvittää, miten kyberturvallisuudesta tehdään ymmärrettävämpää kansalaisille. Siksi myös tämän tutkimuksen aihe valittiin.

Tutkimuksen toimeksiantaja on Digi- ja väestötietovirasto. Digi- ja väestötietoviraston tehtävä on edistää yhteiskunnan digitalisaatiota, näyttää suuntaa ja tehdä Suomesta entistä sujuvammin toimiva yhteiskunta. Tämä on linjassa sen kanssa, mitä opinnäytetyöllä halutaan saavuttaa: ymmärrettävämpää kyberturvallisuutta. Lisäksi opinnäytetyö haluaa näyttää suuntaa kyberturvallisuusalan asiantuntijoille, yrityksille ja organisaatioille.

2 TUTKIMUSSTRATEGIA

Tässä luvussa esitetään tutkimusasetelma ja tutkimuksen tekemisen teoreettinen viitekehys. Alaluvuissa esitellään tutkimuksen tutkimusongelma ja -kysymykset. Sen jälkeen kuvataan tutkimusmenetelmät eli tavat, joilla aineisto kerätään ja analysoidaan. Lisäksi kuvataan, miten tutkimus tullaan toteuttamaan. Lopuksi tarkastellaan tutkimuksen luotettavuuden arviointia.

2.1 Tutkimusongelma

Kyberturvallisuus koskettaa jokaista meistä, ja sen takia sen pitäisi olla myös ymmärrettävää jokaiselle meistä. Tämän takia ymmärrettävämpään kyberturvallisuusviestintään olisi syytä kiinnittää enemmän huomiota. Asioista voidaan

tehdä ymmärrettävämpiä yleistajuistamisen avulla. Kyberturvallisuuden yleistajuistamista ei ole kuitenkaan määritelty, sitä ei ole tutkittu, eikä siihen ole saatavilla keskitetysti ohjeita. Nämä muodostavat tutkimusongelman.

Tutkimuksessa vastataan seuraaviin tutkimuskysymyksiin:

1. Mitä kyberturvallisuuden yleistajuistaminen tarkoittaa?
2. Miten kyberturvallisuudesta tehdään ymmärrettävämpää ja kiinnostavampaa kansalaisille?
3. Kenen vastuulla on, että kansalaiset ymmärtävät kyberturvallisuutta?
4. Minkälainen tarve kyberturvallisuuden yleistajuistamiselle on?

Tutkimusongelmaa voidaan luonnehtia seuraavasti: ilmiötä ei ymmärretä riittävän hyvin. Tätä korostaa se, että kyberturvallisuuden yleistajuistaminen ei ole vakiintunut termi, eikä termillä löydy aiempia tutkimuksia. Tämän takia tutkimuskysymyksissä lähdetään liikkeelle kyberturvallisuuden yleistajuistamisen määrittelemisestä.

Kanasen (2017) mukaan laadullinen tutkimus pyrkii ilmiön syvälliseen ymmärtämiseen. Laadullisen tutkimuksen tavoitteena on kuvata, ymmärtää ja antaa tulkinta tutkittavasta ilmiöstä. Tuomen ja Sarajärven (2018) mukaan laadullinen tutkimus on empiiristä ja siinä tarvitaan teoriaa. Empiirinen tarkoittaa, että ilmiöstä tehdyt havainnot tehdään tutkimusaineistosta. Teorialla viitataan tutkimuksen teoreettiseen viitekehykseen. Teoreettisessa viitekehyksessä luodaan katsaus siihen, miten asiat ovat ja tutkimuksen tuloksissa kuvataan, miten asioiden pitäisi olla tai miten asioiden olisi hyvä olla. Tämän tutkimuksen tavoite on ymmärtää ilmiötä ja antaa tulkinta siitä. Edellä mainittujen takia tutkimuksen tutkimusote on laadullinen tutkimus.

2.2 Tutkimusmenetelmät

Tutkimuksessa toteutetaan ensin kuvaileva kirjallisuuskatsaus, jolla taustoitetaan ilmiötä. Kirjallisuuskatsaus toteutetaan narratiivisena yleiskatsauksena, jonka tarkoitus on tiivistää aiempia aiheesta tehtyjä tutkimuksia (Salminen

2011). Kirjallisuuskatsauksella selvitetään, mitä ilmiöstä tiedetään tällä hetkellä. Kirjallisuuskatsaus toimii myös tutkimusmenetelmänä siinä määrin, että sen avulla määritellään kyberturvallisuuden yleistajuistaminen.

Kirjallisuuskatsauksen jälkeen varsinainen tutkimus tehdään teemahaastatteluilla kerätyllä aineistolla. Tutkimuksen aineisto kerätään teemahaastatteluilla tutkimusongelman luonteen vuoksi: sopivaa olemassa olevaa tietoa ei ole saatavilla, joten ajankohtainen tieto hankitaan kyberturvallisuuden asiantuntijoilta. Tutkimuksessa hyödynnetään siis primääristä, eli tutkimuksen aikana tutkittavasta kohteesta kerättävää, aineistoa (Kananen 2019).

Teemahaastattelu mahdollistaa haastateltavan vapaan puhumisen ja haastattelijan ja haastateltavan vuorovaikutuksen. Teemahaastattelussa käsitellään samoja teemoja ja kysymyksiä kaikkien haastateltavien kanssa. (Vilkka 2021; Tuomi & Sarajärvi 2018.) Haastattelut toteutetaan joko paikan päällä tai etänä. Kanasen (2017) mukaan teemahaastattelutilanne vaatii tutkijan ja haastateltavan fyysistä, samanaikaista läsnäoloa. Tutkimus ei keskity kuitenkaan esimerkiksi haastateltavien puheeseen tai käyttäytymiseen, vaan asiasisältöön. Asiasisältö saadaan irti myös etähaastattelussa. Teemahaastatteluun tulee laatia teemahaastattelurunko, johon käsiteltävät teemat merkitään (Kananen 2017).

Yleistajuistamisen tarpeen selvittäminen asiantuntijoilta voi herättää kritiikkiä: miksi asiaa ei kysytä kansalaisilta? Kansalaisilta kysyminen voisi tarjota aitoja kokemuksia siitä, koetaanko kyberturvallisuus monimutkaiseksi ja vaatiiko se yleistajuistamista. On kuitenkin huomioitava, että kansalaiset muodostavat hyvin monipuolisen ryhmän. Joten jos halutaan luotettava tulos, otoksen pitäisi olla laaja. Tässä tutkimuksessa ei ole mahdollisuutta tähän käytettävissä olevien voimavarojen takia. Tulevissa tutkimuksissa voisi kuitenkin arvioida ja syventää tämän tutkimuksen tuloksia kansalaisten näkemyksien avulla.

Haastateltavat asiantuntijat tulevat edustamaan monipuolisesti kyberturvallisuusalaa, joten heidän näkökulmansa ilmiöön oletetaan kattavaksi. Tässä yhteydessä on kuitenkin syytä tiedostaa, että moni haastateltavista tekee työssään yleistajuistamista. Tämä voi vaikuttaa heidän objektiivisuuteensa, kun he arvioivat yleistajuistamisen tarvetta. Tutkimuksessa tiedostetaan, että tulokset

heijastavat nykypäivän asiantuntijoiden näkemyksiä ja haastateltavien ammatillinen tausta saattaa vaikuttaa tuloksiin.

Aineiston analyysimenetelmät

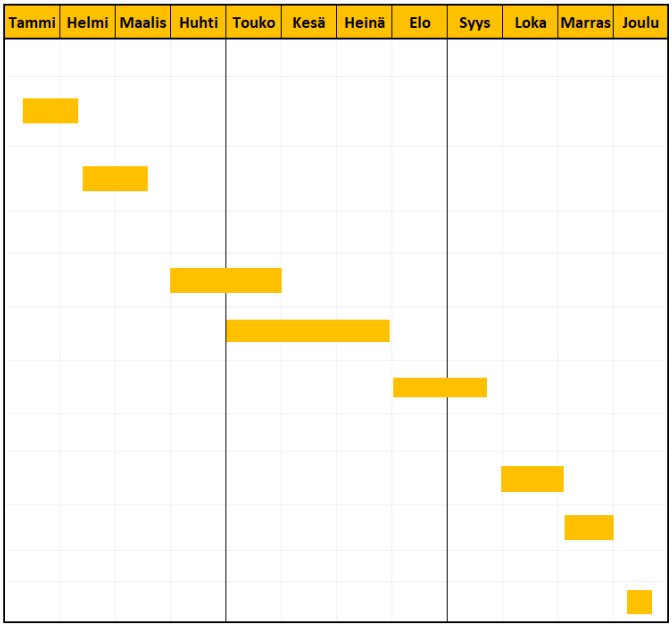
Teemahaastattelun aineisto analysoidaan sisällönanalyysillä. Tuomi ja Sarajärvi (2018, luku 4) kuvaavat, että sisällönanalyysin tavoite on tiivistää selkeä kuvaus tutkittavasta ilmiöstä. Tutkijan tehtävä on löytää aineistosta tutkimusongelman kannalta oleellisia kohtia. Näitä kerätään, yhdistetään ja niiden avulla luodaan päätelmiä ilmiöstä. Vilkka (2021) kuvaa kaksi sisällönanalyysin toteutustapaa: teoria- ja aineistolähtöinen sisällönanalyysi. Teorialähtöinen tarkoittaa, että aineisto analysoidaan jonkin olemassa olevan teorian pohjalta. Aineistolähtöinen tarkoittaa, että analysointi tapahtuu aineiston ehdoilla – tavoitteena on löytää esimerkiksi jonkinlainen tyypillinen kertomus aineistosta.

Koska aiempaa tietoa on hajanaisesti saatavilla, analyysin perustaminen olemassa olevaan teoriaan ei ole mielekästä. Tämän vuoksi valitaan aineistolähtöinen sisällönanalyysi. Analyysissä on kolme vaihetta: 1) pelkistäminen, 2) ryhmittely ja 3) käsitteellistäminen. Pelkistämisessä aineistosta karsitaan tutkimusongelman kannalta epäolennainen tieto. Tämän jälkeen tieto ryhmitellään uudeksi kokonaisuudeksi. Lopuksi ryhmät käsitteellistetään eli nimetään ryhmien sisältöä kuvaavalla käsitteellä. Käsitteellistämistä jatketaan, kunnes on päästy aineistoa kuvaavaan yhteen käsitteeseen. Näiden kautta syntyy tutkimuksen tuloksia, jotka selittävät tutkittavaa ilmiötä. (Vilkka 2021; Tuomi & Sarajärvi 2018.)

2.3 Tutkimuksen vaiheet

Tutkimuksen aikataulu näkyy kuvassa 1. Tutkimuksen tekeminen on jaettu kolmeen vaiheeseen, joita seuraa lopetus eli tutkimuksen valmistuminen. Tutkimuksen toteuttamiseen on varattu yhteensä 11 kuukautta aikaa.

Työvaihe	Aloitus	Lopetus
VAIHE 1		
Johdannon ja tutkimusasetelman kirjoittaminen	11.1.2023	11.2.2023
Teoreettinen viitekehys, kirjallisuuden hankinta	13.2.2023	13.3.2023
VAIHE 2		
Teemahaastattelut	1.4.2023	31.5.2023
Aineiston läpikäyminen ja tutkimuksen kirjoittaminen	1.5.2023	31.7.2023
Tulokset ja jatkokehitys	1.8.2023	24.9.2023
VAIHE 3		
Työn viimeistely	1.10.2023	5.11.2023
Työn lopputarkastus	6.11.2023	26.11.2023
LOPETUS		
Työ on valmis viimeistään	11.12.2023	



Kuva 1 Tutkimuksen aikataulu

Ensimmäisessä vaiheessa (tammikuu–maaliskuu) laaditaan tutkimussuunnitelma, johon sisältyy johdanto, tutkimusasetelma ja teoreettinen viitekehys. Lisäksi hankitaan tarvittavaa kirjallisuutta. Toisessa vaiheessa (huhtikuu–syyskuu) toteutetaan teemahaastattelut ja analysoidaan niiden tulokset. Lisäksi kirjoitetaan tutkimustulokset, johtopäätökset ja pohdinta. Kolmannessa vaiheessa (lokakuu–marraskuu) työ viimeistellään ja se tarjotaan lopputarkastukseen. Tutkimus on valmis 11.12.2023 mennessä.

Haastateltavien valinta

Haastateltavien valinta tulee olla huolellisesti tehty tutkimustavoitteen mukaisesti (Vilkka 2021). Tuomi ja Sarajärvi (2018) korostavat, että haastateltavat tulee valita harkiten ja valinnan tulee olla tarkoitukseen sopivaa. Nämä asiat huomioidaan tutkimuksessa. Haastateltavien valinnassa käytetään harkinnanvaraista otosta. Tällä tarkoitetaan sitä, että haastateltavat valitaan tutkijan asettamien kriteerien perusteella (Tietoarkisto 2021). Kriteeri on, että valittavan asiantuntijan tulee edustaa monipuolisesti kyberturvallisuusalaa.

Vilkka (2021) ja Kananen (2017) korostavat, ettei haastateltavien määrää voi tietää etukäteen. Haastateltavia on tarpeeksi silloin, kun uuden haastateltavan vastaukset eivät tuo uutta tietoa aineistoon. Tällöin haastateltavien määrä on

saturoitunut eli kyllääntynyt. Tuomi ja Sarajärvi (2018) huomauttavat, ettei aineiston kyllääntymiseen vetoaminen sovi kaikkiin laadullisiin tutkimuksiin. Haastateltavien määrä halutaan tutkimuksessa pitää mahdollisimman pienenä. Ei sen takia, että pieni haastateltavien joukko olisi parempi – kuten Kananen ja Vilkka huomauttavat – vaan sen takia, että jokaisen haastateltavan pitää tuoda erilainen näkökulma ilmiöön.

Haastatteluaineiston käsitteleminen

Haastattelut nauhoitetaan ja nauhoitettu puhe litteroidaan, eli puhe kirjoitetaan tekstiksi. Vilkan (2021) mukaan litteroinnin tarkkuuteen vaikuttaa tutkimuksen tavoite ja tutkimuksessa käytetyt lähestymistavat. Kanasen (2017) mukaan usein litterointiin riittää lauseen sanoman tiivistäminen niin, että vastaajan koko ilmaisua ei tuoda esille. Haastatteluille tehdään Hirsjärven ja Hurmeen (2022) kuvaama sanatarkka litterointi, eli puhe kirjoitetaan tekstiksi sanasta sanaan. Litterointiin ei kuitenkaan oteta mukaan esimerkiksi taukoja tai sanojen painotuksia. Mahdolliset toistot ja täytesanat jätetään pois tutkimusaineiston esittelyssä selkeyden takia.

Haastatteluaineistoa käytetään vain tähän tutkimukseen ja se poistetaan tutkimuksen julkaisemisen jälkeen. Opinnäytetyön aineisto ei ole yhteiskunnallisesti merkittävää, joten tutkimuksen jälkeinen säilyttäminen ei ole tarpeellista. Haastatteluaineistojen analyysit anonymisoidaan. Niiden perusteella ei siis voi tunnistaa haastateltavia tai heidän edustamiaan yrityksiä. Jokaisesta haastateltavasta kirjoitetaan kuvaus, jossa avataan haastateltavan asiantuntijuutta yleisesti. Kuvaukset varmistetaan haastateltavilta.

Kysymykset tarjotaan haastateltaville etukäteen, jotta heillä on mahdollisuus valmistautua niihin. Haastattelut toteutetaan tutkimuseettisten periaatteiden mukaan, ja tutkimus noudattaa Tutkimuseettisen neuvottelukunnan (2023) hyvän tieteellisen käytännön ohjeistusta. Haastateltaville kerrotaan kaikki tarvittavat tiedot haastattelusta ja aineiston käsittelemisestä (Ranta & Kuula-Lummi 2017). Haastateltava voi kieltäytyä haastattelusta tai kieltää aineiston käsitteleminen, milloin vain ennen tutkimuksen julkaisua (Kananen 2017).

2.4 Luotettavuusvarauma

Seuraavaksi esitetään, miten tämän tutkimuksen luotettavuutta arvioidaan. Esitettyihin asioihin palataan pohdintaluvun luotettavuustarkastelussa. Tuomi ja Sarajärvi (2018) ja Kananen (2017) nostavat esille, että laadullisen tutkimuksen luotettavuuden tarkasteluun ei ole yksiselitteistä vastausta. Vastaus riippuu pitkälti oppaasta, jota tutkija tarkastelee. Vilkan (2021) mukaan laadullisen tutkimuksen luotettavuus perustuu lopulta tutkijaan ja hänen rehellisyyteensä. Kananen (2017) kuvaa kaksi yleistä tieteellisen tutkimuksen luotettavuuden mittaria: reliabiliteetti ja validiteetti.

Kanasen (2017) mukaan reliabiliteetti tarkoittaa, että uusintasuorituksessa päädytään samankaltaisiin tuloksiin kuin alkuperäisessä tutkimuksessa. Validiteetti tarkoittaa, että tutkimuksessa tutkitaan oikeita asioita oikealla tavalla. Validiteetti tulee huomioida esimerkiksi tutkimusotteen ja -menetelmien kohdalla. Reliabiliteetti ja validiteetti nähdään kuitenkin monesti määrällisen tutkimuksen arviointitapoina (Vilkka 2021; Tuomi & Sarajärvi 2018). Toisaalta Tuomi ja Sarajärvi (2018) korostavat, ettei tarkkojen termien määrittely ole yhtä mielekästä kuin se, mitä niillä tarkoitetaan. Kananen (2017) ottaa tämän huomioon sanomalla, että käsitteet ovat kyllä käytössä määrällisessä tutkimuksessa, mutta niiden sisältö on määritelty eri tavalla siinä yhteydessä.

Vilkka (2021) kirjoittaa, että laadullisen tutkimuksen tulokset eivät ole käytännössä toistettavia (reliabiliteetti), koska jokainen tutkimus on ainutkertainen. Tuloksien luokittelussakin tutkijat voivat päätyä erilaisiin tulkintoihin, vaikka luokittelu- ja tulkintasäännöt olisi esitelty perusteellisesti. Eri tutkijoiden tulisi kuitenkin samoilla luokittelu- ja tulkintasäännöillä löytää muiden tulkintojen ohella myös se, jonka tutkimuksen tekijä on esittänyt.

Hirsjärvi ja Hurme (2022) nostavat esiin reliabiliteetin ongelmallisuuden teemahaastattelun luotettavuuden arvioinnissa. Heidän mukaansa on epätodennäköistä, että samalta haastateltavalta saisi saman tuloksen eri haastattelukerroilla. Tämä johtuu siitä, että ihmisillä on taipumus muuttua ajan kuluessa. Näiden perusteella reliabiliteettia ei oteta luotettavuuden arviointiin mukaan.

Tutkijan luotettavuus

Vilkan (2021) mukaan keskeistä on tutkijan luotettavuus, koska luotettavuuden arvioinnissa keskitytään tutkijan tekemiin valintoihin, ratkaisuihin ja tekoihin. Luotettavuuden arviointi kulkee koko tutkimuksen läpi ja tutkija tekee sitä jokaisen valinnan kohdalla. Edellä mainittu liittyy Kanasen (2017) kuvaamaan arvioitavuuteen, eli tutkimuksen dokumentaation tulisi olla riittävä. Dokumentaation avulla lukijan pitää voida jäljittää ja arvioida tutkijan tekemät valinnat. Myös Hirsjärvi ja Hurme (2022) korostavat riittävän dokumentaation tärkeyttä luotettavuuden tarkastelussa.

Tutkimuksessa tähdätään siihen, että tutkijan tekemät valinnat ovat läpinäkyviä, suunniteltuja ja ne perustellaan lukijalle. Tutkimus on tutkijan ensimmäinen. Tutkija tiedostaa tämän takia, että virheet ovat mahdollisia ja valintoja tulee tehdä harkitusti. Luotettavuutta parantaakseen tutkija tutustuu huolellisesti tutkimuskirjallisuuteen ja hakee opinnäytetyön ohjaajilta aktiivisesti tukea. Tutkija on esimerkiksi antanut opinnäytetyön ohjaajille mahdollisuuden ehdottaa haastateltavia tutkimukseen. Tällä tavalla haastateltavien joukko ei ainoastaan ole tutkijan valitsema. Tutkimukseen on myös varattu reilusti aikaa, jotta tutkijan on mahdollista perehtyä tutkittavaan ilmiöön riittävän syvällisesti.

Menetelmien luotettavuus

Tutkimuksessa tulee tutkia oikeita asioita oikealla tavalla. Tutkimuksen validiteetin tulee siis olla kunnossa. Kananen (2017) toteaa, että laadullisen tutkimuksen luotettavuutta voidaan parantaa vahvistettavuuden avulla. Tämä tarkoittaa, että tietoa kerätään eri lähteistä ja kerättyä tietoa verrataan keskenään. Tämä toteutetaan aineistotriangulaation avulla, eli tutkimuksessa hyödynnetään useampaa aineistonkeruumenetelmää. Kahdella tavalla kerätyn aineiston tarkoitus on vähentää virheiden ja väärien yleistysten mahdollisuutta. Tuomen ja Sarajärven (2018) mukaan monimenetelmällisyys validiteettikriteerinä ei ole kuitenkaan ongelmaton. He tuovat esiin kaksi keskustelua, joita monimenetelmällisyydestä käydään. Ensimmäisen mukaan monimenetelmällisyydessä olisi kyse menetelmien vertailusta, eli selvitetään, mikä menetelmä antaa oikean tuloksen. Toisen mukaan monimenetelmällisyyden tavoitteena olisi lisätä tutkimuksen leveyttä ja syvyyttä, ei sen luotettavuutta.

Tuomen ja Sarajärven (2018) mukaan on tärkeä miettiä, annetaanko haastateltavien tutustua tuloksiin ennen kuin ne julkaistaan. Haastateltaville tarjotaan tässä tutkimuksessa mahdollisuus tutustua tutkijan tekemiin tulkintoihin. He voivat tarkistaa analyysit ja vaatia oikaisua niihin. Tätä toimintatapaa kutsutaan myös osallistujatarkistukseksi. Sen tavoitteena on tulkintojen uskottavuuden määritteleminen (Hirsjärvi & Hurme 2022). Tällä pyritään myös karsimaan vääriä tulkintoja haastateltavien sanomisista. Aineiston analysoinnin näkökulmasta tulee muistaa, että teemahaastattelun tuloksiin liittyy aina tulkintaa (Hirsjärvi & Hurme 2022).

3 TEOREETTINEN VIITEKEHYS

Tässä luvussa esitetään tutkittavan ilmiön taustaa avaava teoreettinen viitekehys. Alaluvuissa tarkastellaan ymmärrettävää viestintää ja aiempia kyberturvallisuuden ja tieteen yleistajuistamisen tutkimuksia. Kyberturvallisuus määritellään Turvallisuuskomitean (2018) sanaston määritelmän mukaisesti: kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kybertoimintaympäristö tarkoittaa käytännössä digitaalista toimintaympäristöä.

On hyvä huomioida, että esimerkiksi Suomen vuoden 2019 kyberturvallisuusstrategiassa ja Sanastokeskuksen TEPA-termipankissa hyödynnetään Turvallisuuskomitean sanaston määritelmää. Turvallisuuskomitean määritelmä nostetaan esille myös Cyber Citizen -kyberkansalaistaitohankkeessa (Limnéll ym. 2023). Turvallisuuskomitean käyttämä määritelmä on laajasti käytössä, joten sitä hyödynnetään myös tässä tutkimuksessa.

3.1 Ymmärrettävä viestintä

Tämä alaluku käsittelee ymmärrettävän viestinnän teemoja ja asiantuntijaviestintää. Viestintä on ihmisen toiminnan perusta ja se mahdollistaa organisoidun tekemisen. Ytimessään se on vuorovaikutusta toisen ihmisen kanssa. Vuorovaikutuksessa keskeistä on se, millä tavalla asioista viestitään kielellisesti ja ei-kielellisesti. Ei-kielellisyys viittaa niihin viestinnän muotoihin, jotka eivät ole peräisin kielestä tai sanallisista ilmaisuista – esimerkiksi eleet, ilmeet ja ää-

nenpainot. Tiedottamisesta puhutaan, kun viitataan suoraviivaiseen lähettäjältä vastaanottajalle tapahtuvaan viestintää. Viestintä ei ole kuitenkaan suoraviivaista tiedottamista, eikä voida ajatella, että tietoa vain välitetään ja vastaanottaja toimii halutulla tavalla. (Juholin 2022.)

Juholinin (2022) mukaan viestinnän tehokkuuteen vaikuttaa moni asia: kuinka hyvin viesti saavuttaa oikeat tahot, kuinka kiinnostava viesti on ja millaiseen ympäristöön viesti välitetään. Lisäksi voi olla, ettei vastaanottaja ymmärrä viestiä. Viestinnän haluttuun lopputulokseen vaikuttaa se, miten hyvin vastaanottaja ymmärtää viestin.

Selkokieli, yleiskieli ja erikoiskieli

Käytettävä kieli voidaan jakaa kolmeen kielimuotoon: 1) selkokieli, 2) yleiskieli ja 3) erikoiskieli. Selkokieli tarkoittaa muotoa, jossa sisältöä, sanastoa ja kielen rakennetta on muokattu yleiskieltä yksinkertaisemmaksi. Yleiskieli tarkoittaa muotoa, jossa viestintä suunnataan suurelle joukolle. Erikoiskieli tarkoittaa muotoa, joka on tietyn ryhmän ymmärrettävissä. Erikoiskielet ovat rakenteeltaan ja sisällöiltään vaikeita ja niihin sisältyy omaa sanastoa. (Leskelä ja Uotila 2020; Erikoiskieli s.a.; Selkokieli s.a.; Yleiskieli s.a.) Kyberturvallisuus on erikoiskieli, se on siis kielellisesti poissulkeva. Tämän takia kohderyhmän ei voi olettaa automaattisesti ymmärtävän sitä.

Asiantuntijaviestintä

Juholin (2022) toteaa, että työyhteisöviestintä on viestintää, joka ulottuu työyhteisön sisälle ja sen ulkopuolelle. Työyhteisöviestintä on taito, joka sisältää työn kannalta oleellisen tiedon jakamista. Päivittäisviestintä on termi, jolla Juholin viittaa tehtäväkohtaiseen päivästä toiseen tapahtuvaan tiedon jakamiseen. Päivittäisviestintä on sidoksissa siihen, mitä asiantuntija päivittäin tekee. Juholinin mukaan asiantuntijan tulee hallita alansa ja hänellä tulee olla viestintäosaamista. Viestintäosaaminen sisältää tietoja ja taitoja, kuten puhumista ja kirjoittamista.

Välillä viestintä on velvollisuus. Näin on esimerkiksi EU:n yleisen tietosuoja-asetuksen (GDPR) ja esteettömyysdirektiivin kohdalla. GDPR velvoittaa selkeään viestintään ja esteettömyysdirektiivi säätelee viranomaisten ja yksityisen sektorin digitaalisten palveluiden saavutettavuutta. (Juholin 2022.) Myös ymmärrettävä viestintä voi olla velvollisuus, näin on, kun puhutaan virkakielestä. Hallintolain 9. pykälän mukaan virkakielen tulee olla asiallista, selkeää ja ymmärrettävää. (Tiililä 2015.) Tämä tarkoittaa sitä, että viranomaisten Suomessa tulee huomioida ymmärrettävyys omassa kyberturvallisuusviestinnässään.

Kohderyhmälähtöinen viestintä

Juholinin (2022) mukaan seuraukset voivat olla kovia, jos viestintä epäonnistuu, viesti torjutaan tai se ymmärretään väärin. Tämän takia viestinnältä vaaditaan selkeyttä ja ymmärrettävyyttä. Viestinnän vaikuttavuutta voidaan parantaa ymmärtämällä vastaanottajan tilanne, tarpeet ja odotukset. Kaikille ihmisille ei voi viestiä samalla tavalla.

Mustajoki (2013) korostaa kohderyhmälähtöisyyttä. Sillä on merkittävä rooli, kun tieto halutaan saada ihmisten ulottuville. Viestijän tulee käyttää oikein muotoiltuja sanoja, jotta viestintä ymmärretään oikein. Myös Haney ja Lutters (2018) kirjoittavat kohderyhmälähtöisestä viestinnästä. He toteavat, että kun kyberturvallisuuden asiantuntijat kouluttavat, heidän on ymmärrettävä kohderyhmänsä.

Kyky sopeuttaa puhe ja teksti tilanteen mukaiseksi on merkittävää kommunikaatiotaidoissa. Monesti tämä kuitenkin menee pieleen ja meidän on Mustajoen (2013) mukaan tutkitustikin vaikea asettua toisten ihmisten asemaan. Vastaanottajan tietotaito arvioidaan usein samanlaiseksi kuin oma tietotaito, vaikka näin ei olisi.

3.2 Tieteen yleistajuistaminen

Tässä alaluvussa tarkastellaan tieteen yleistajuistamista ja tutustutaan tutkimuksiin, joissa tiedettä on yleistajuistettu. Tieteen yleistajuistaminen tarkoittaa Strellmanin ja Vaattovaaran (2013) mukaan sitä, että vuorovaikutus onnistuu

muidenkin kuin samalla tieteenalalla toimivien kanssa. Raevaaran (2016) mukaan tieteen yleistajuistaminen tarkoittaa sellaista sisältöä, joka perustuu tutkittuun tietoon, mutta jota viedään muille kuin alan tutkijoille.

Strellmanin ja Vaattovaaran (2013) mukaan tieteen yleistajuistamista tekevän tehtäviin kuuluu viestintä tiedeyhteisön sisällä ja sen ulkopuolella. Tapa, jolla tieteestä kerrotaan, riippuu kontekstista ja kohderyhmästä. On eroa, yleistajuistetaanko asiaa esimerkiksi akateemiselle yleisölle vai suurelle yleisölle. Strellmanin ja Vaattovaaran mukaan on keskeistä miettiä, kenen vastuulla yleistajuistaminen on.

Raevaaran (2016) mukaan on erilaisia yleistajuisuuden tasoja, jotka riippuvat siitä, kuinka kaukana kohderyhmä on tutkijoista. Etäisyys määrittelee sen, kuinka paljon yleistajuistamista tehdään. Kun puhutaan suuresta yleisöstä eli kansalaisista, on myös huomioitava, että joukko koostuu erilaisista yksilöistä.

Näin tiedettä on yleistajuistettu

Seuraavaksi tarkastellaan kahta tutkimusta, joissa tieteen yleistajuistamista on tutkittu. Tero Linjama (2018) tutki yleistajuistamista hoitotyötätekeville. Opinnäytetyössä tutkittiin, miten lääketieteen tietoa yleistajuistetaan terveydenhuollon ammattilaisille. Tutkimuksessa tutkittiin alan artikkeleita, joissa arvioitiin esimerkiksi yleistajuistamisen piirteitä ja mietittiin median käyttöä. Tulokset viittaavat siihen, että kohderyhmän huomioiminen on keskeistä yleistajuistamisessa. Viestijän tulee huomioida vastaanottajan ominaisuudet ja ymmärryksen rajallisuus. Lisäksi yleistajuistamisessa keskeistä on asian tiivistäminen ja olennaisen poimiminen.

Nelli Miettinen (2016) tutki lääketieteen popularisointia mediassa. Maisterintutkielmassa tutkittiin teksti- ja haastatteluaineistojen kautta kielen käyttämistä, kun lääketiedettä yleistajuistetaan mediassa. Tulokset viittaavat siihen, että erilaiset kielenkäytön keinot ovat keskeisiä yleistajuistamisessa. Merkittävää on myös taito korostaa ja pelkistää asioita. Molemmissa tutkimuksissa nousi esille samoja tuloksia, kuten kyky korostaa kohderyhmälle oleellinen asia.

3.3 Kyberturvallisuuden yleistajuistaminen

Yleistajuinen ja kansantajuinen nähdään monesti synonyymeinä. Strellman ja Vaattovaara (2013) kirjoittavat kuitenkin termien sävyerosta: kansantajuinen tarkoittaa koko kansan ymmärrettävää muotoa, kun taas yleistajuisella halutaan estää tiedon viemistä yhteiskunnassa “ylhäältä alaspäin”. Vastaavasti Raevaara (2018) toteaa, että kansantajuinen terminä on aikansa elänyt; ennen vanhaan "rahvasta" piti valistaa. Kielitoimiston sanakirjassa (2016) kansantajuinen määritellään: *helppo-, yleistajuinen*. Yleistajuinen määritellään: *helppo-, kansantajuinen, populaari*. Yleistajuiseen otetaan populaari mukaan ja näiden huomioiden takia yleistajuinen valittiin.

Kyberturvallisuuden yleistajuistaminen tarkoittaa tutkimuksessa sitä, että kyberturvallisuudesta viestitään ymmärrettävästi ja viestintä räätälöidään sen mukaan, kenelle puhutaan. Viestinnän tulee olla kohderyhmälähtöistä, ja kohderyhmän tulee kyetä ymmärtämään viesti riippumatta omista lähtökohdistaan. Yleistajuistamisella ei tarkoiteta, että viesti olisi jokaisen kansalaisen ymmärrettävissä, vaan se on kohderyhmän ymmärrettävissä.

Määritelmässä nojataan tässä luvussa aiemmin esitettyihin kohderyhmälähtöisen viestinnän ja tieteen yleistajuistamisen määritelmiin. Kyberturvallisuuden yleistajuistamisesta tehdään käsite, jonka alle kootaan yleistajuistamisen toimintatavat. Käsitteen määrittelemisen avulla halutaan myös tehdä asiaan tutustumisesta helpompaa kyberturvallisuuden asiantuntijoille.

3.4 Näin kyberturvallisuuden viestintää on tutkittu

Tässä alaluvussa tutustutaan aiempiin kyberturvallisuuden viestintää käsitteleviin tutkimuksiin. Lotta Sandroos (2021) tutki pro gradu -tutkielmassaan yksityishenkilöille kohdistettua tietoturvaviestintää Kyberturvallisuuskeskuksen tuottaman aineiston kautta. Aineistoja analysoitiin kehysanalyyttisellä menetelmällä, eli aineistosta tunnistettiin viestinnällisiä kehyksiä. Viestinnälliset kehykset viittaavat viestinnän taustalla oleviin rakenteisiin, joiden pohjalta viestintää tehdään. Sandroos tunnisti kaksi kehystä: sosiaaliseen markkinointiin pohjautuvan yhteiskunnallisen ulottuvuuden kehyksen ja suojelumotivaatioteoriaan pohjautuvan uhkapuheen kehyksen.

Sandroosin (2021) tutkimuksen keskeisimmät tulokset liittyvät sosiaaliseen markkinointiin ja pelottelupuheeseen. Sosiaalisessa markkinoinnissa ideana on tarjota palkinto käyttäytymisen muutoksesta. Pelottelupuheessa keskeistä on uhkakuvien kautta vaikuttaa kohderyhmän käyttäytymiseen. Sandroos toteaa, että pelottelupuhe on yleistä ja korostaa, että liika pelottelupuhe voi kääntyä itseään vastaan. Ihmisten käytökseen vaikuttaminen tulisi tehdä rohkaisemisen kautta.

Sandroos (2021) kirjoittaa tutkimuksessaan myös kansalaisten kouluttamisen vastuukysymyksestä. Suomessa ei ole tarkkaa tahoa tälle; Kyberturvallisuuskeskus tekee tätä kyllä, mutta onko se tehokasta? Tutkimuksessa ei vastata tähän. Tutkimuksen mukaan samaa koulutusmateriaalia ja samanlaista viestintää ei voida käyttää kaikille. Myös Haney ja Lutters (2018) tuovat esille ajattelutavan heikkouden. Sen sijaan tulisi siirtyä toimivampaan, kohderyhmän huomioon ottavaan viestintään (Sandroos 2021; Haney ja Lutters 2018).

3.5 Kyberturvallisuus on jokaisen asia

Tässä alaluvussa tarkastellaan sitä, miten kyberturvallisuus koskettaa jokaista meistä. ENISAn eli Euroopan unionin kyberturvallisuusviraston (2021) julkaisussa korostetaan kyberturvallisuuden merkitystä kansalaisille ja nostetaan kyberturvatietoisuuden heikko nykytila esille. Kyberturvallisuudesta ollaan kyllä tietoisia, mutta turvallisten toimintatapojen noudattaminen on vaikeaa. Kansalaisten tulisi yhä paremmin ymmärtää kyberturvallisuutta. Myös valtio on tunnistanut kyberturvallisuuden merkityksen kansalaisten elämässä. Suomen kyberturvallisuusstrategia mainitsee: kansallisesti on varmistettava, että jokaisella on riittävät valmiudet toimia turvallisesti digitaalisessa toimintaympäristössä (Turvallisuuskomitea 2019).

Cyber Citizen -hankkeessa tutkittiin EU:n jäsenmaiden kyberkansalaistaitojen opettamisen nykytilaa ja opetussisältöjä, joita taitojen opettamiseen on olemassa. Tutkimuksen mukaan kansalaisten kyberturvallisuuden perusosaaminen vaihtelee suuresti eri maiden kesken. Keskeinen tulos on, että EU:n jäsenmailla on tahto kehittää kansalaisten kyberkansalaistaitoja. Lisäksi jäsenmaissa ollaan siirtymässä pois ajatuksesta, että kyberturvallisuus olisi pelkästään ammattilaisten vastuulla. Sen sijaan digitalisaation ja sen turvallisuuden

nähdään olevan erottamaton osa ihmisten, organisaatioiden ja yhteiskuntien toimintaa. (Limnéll ym. 2023.)

Kyberturvallisuus nähdään kansalaistaitona

Lehdon ym. (2017) tutkimuksessa todetaan, että jokaisen suomalaisen on tunnistettava ja ymmärrettävä oma roolinsa turvallisuustoimijana. Samassa tutkimuksessa sanotaan, että kyberturvallisuuden pitäisi olla peruskansalaistaito Suomessa. Cyber Citizen -hankkeen tutkimuksen mukaan kyberkansalainen on EU:n alueella tilapäisesti tai vakituisesti oleva henkilö, joka käyttää digitaalisia palveluita tai hyötyy niiden tuottamisesta. Kyberkansalaistaito määriteltiin kybertoimintaympäristössä tarvittavien tietojen, taitojen ja kykyjen yhdistelmäksi. (Limnéll ym. 2023.)

Megatrendit ennakoivat tulevaa

Kyberturvallisuus on jokaisen asia. Tämä johtuu osaltaan myös digitalisaatiosta, eli tietotekniikan yleistymisestä kansalaisten arkielämässä ja yhteiskunnassa. Tämä kehitys alkoi vuosikymmeniä sitten, eikä se osoita hidastumisen merkkejä. (Dufva 2023.) Seuraavaksi tarkastellaan muutamaa megatrendijulkaisua. Megatrendi tarkoittaa laajaa muutoksen kaarta, eli suuria kansainvälisiä ilmiöitä, jotka pysyvät samanlaisina pitkään.

Sitra eli Suomen tulevaisuustalo korosti vuoden 2020 megatrendilistauksessa, että tulevaisuudessa teknologia sulautuu kaikkeen. Tällä tarkoitetaan teknologian nopeaa kehitystä ja uusien sovelluksien käyttöönottoa. Vuoden 2023 listauksessa megatrendiksi nostettiin se, että kilpailu digivallasta kiihtyy. Molemmissa listauksissa todettiin, että teknologian ymmärtäminen korostuu tulevaisuudessa. Tämä johtuu siitä, että yksilöiden ja yhteiskuntien tulee ottaa haltuun uudenlaisia digi- ja teknologiataitoja, kun yhä useampi asia tapahtuu digitaalisilla alustoilla. (Dufva 2023; Dufva 2020.)

3.6 Yhteenveto

Ymmärrettävä viestintä -alaluvussa tarkasteltiin erilaisia ymmärrettävän viestinnän teemoja ja asiantuntijaviestintää. Luvussa todettiin, että viestinnän rooli on nykypäivänä tärkeä. Viestintä on osa asiantuntijoiden päivittäistä tekemistä ja joskus se on velvollisuus. Kieli jaettiin kolmeen kielimuotoon: 1) selkokieli, 2) yleiskieli ja 3) erikoiskieli. Kyberturvallisuus on erikoiskieli, eli se on kielellisesti poissulkeva. Kohderyhmälähtöinen viestintä korostui aineistosta.

Tieteen yleistajuistaminen -alaluvussa tarkasteltiin tieteen yleistajuistamista. Tieteen yleistajuistamisella tarkoitetaan sitä, että tutkittuun tietoon pohjautuvaa tietoa viestitään muille kuin alan tutkijoille ymmärrettävästi. Lisäksi alaluvussa tutustuttiin kahteen aiempiin aihetta käsitteleviin tutkimuksiin. Tutkimuksissa korostui esimerkiksi oleellisen asian viestiminen kohderyhmälle.

Kyberturvallisuuden yleistajuistaminen -alaluvussa määriteltiin kyberturvallisuuden yleistajuistaminen. Kyberturvallisuuden yleistajuistaminen tarkoittaa sitä, että kyberturvallisuudesta viestitään ymmärrettävästi ja viestintä räätälöidään sen mukaan, kenelle puhutaan. Yleistajuistamisesta tehdään kattotermi, joka kokoaa alleen ymmärrettävän kyberturvallisuuden toimintatavat.

Näin kyberturvallisuuden viestintää on tutkittu -alaluvussa tarkasteltiin Lotta Sandroosin pro gradu -tutkielmaa, jossa hän käsitteli yksityishenkilöille suunnattua tietoturvaviestintää Kyberturvallisuuskeskuksen aineiston kautta. Tutkimuksen keskeiset tulokset liittyvät sosiaaliseen markkinointiin ja pelottelupuheeseen. Sosiaalisessa markkinoinnissa vastaanottajan käyttäytymistä pyritään muuttamaan palkinnon avulla ja pelottelupuheessa käyttäytyminen pyritään muuttamaan uhkakuvien avulla.

Kyberturvallisuus on jokaisen asia -alaluvussa tarkasteltiin, miten kyberturvallisuus koskettaa jokaista meistä. Kyberturvallisuus nähtiin myös kansalaistaitona. Esimerkiksi Cyber Citizen -kyberkansalaistaitohanke kehittää EU:n jäsenmaiden kansalaisten kyberkansalaistaitoja. Hankkeen tutkimuksessa tutkittiin jäsenmaiden kyberkansalaistaitojen opetuksen nykytilaa ja olemassa olevia opetussisältöjä. Luvussa tarkasteltiin myös Sitran megatrendijulkaisuja, joiden mukaan teknologian ymmärtäminen korostuu tulevaisuudessa.

4 TUTKIMUKSEN TEKEMINEN

Tässä luvussa esitetään, miten tutkimustuloksiin päädyttiin. Kuvassa 2 näkyy tutkimusaineiston keräämisen ja analysoimisen vaiheet. Vaiheita on yhteensä yhdeksän ja vaiheet suoritettiin järjestyksessä nuolien mukaan.

Kuva 2 Aineiston keräämisen ja analysoimisen vaiheet

Ensin haastateltaville lähetettiin kutsut haastatteluihin. Kutsut lähetettiin kolmen kuukauden aikana 11:lle haastatteluehdokkaalle alkaen vuoden 2022 joulukuusta. Kaikki paitsi yksi hyväksyi haastattelukutsun – tämä yksi ohjasi aikataulukiireiden takia toisen asiantuntijan suuntaan (H5), joka hyväksyi haastattelukutsun. Haastateltavien määrä oli siis lähes suunnitellun mukainen, vain yksi ehdokas jäi alkuperäisestä suunnitelmasta puuttumaan. Teemahaastattelut pidettiin vuoden 2023 huhtikuun ja toukokuun aikana. Teemahaastattelut tallennettiin, jonka jälkeen ne litteroitiin eli kirjoitettiin tekstiksi. Puhe kirjoitettiin tekstiksi sanasta sanaan.

Litteroinnin jälkeen alkoi aineistolähtöinen sisällönanalyysi, joka koostui Vilkan (2021) sekä Tuomen ja Sarajärven (2018) kuvaamista kolmesta vaiheesta: 1) pelkistäminen, 2) ryhmittely ja 3) käsitteellistäminen. Pelkistämisessä litteroidut aineistot tiivistettiin. Ensin aineistot värikoodattiin, eli aineistoista korostettiin eri väreillä tutkimuskysymysten kannalta oleelliset tiedot – esimerkiksi

ne kohdat korostettiin keltaisella, joissa käsiteltiin ymmärrettävyyden lisäämistä. Tämän jälkeen värikoodatut kohdat siirrettiin toisiin tiedostoihin.

Haastateltavat anonymisoitiin eli heidän nimensä sijasta käytettiin tunnistetta HX, jossa ”H” tarkoittaa haastateltavaa eli on lyhenne, ja ”X” tarkoittaa, monesko haastattelu oli kyseessä. Tunnisteet kulkivat sisällönanalyysin vaiheiden läpi haastateltavan koko litteroidusta puheesta irrotettujen ja värikoodattujen tekstien mukana. Tämän avulla varmistettiin, että ilmaisut ovat aitoja ja niiden asiayhteyteen voitiin palata myöhemmin. Irrottamisen jälkeen tekstien tiivistämistä jatkettiin. Nyt värikoodattujen tekstien ydinidea pelkistettiin eli kirjoitettiin uudestaan tiiviimpään muotoon (Vilkka 2021).

Seuraavaksi esitetään esimerkki pelkistämisestä:

> H1: Pitää ymmärtää se, kenelle puhutaan koska jos ei sitä ymmärrä niin sitten saattaa useasti valitettavasti mennä siihen, että käyttää vaikka liian vaikeita sanoja tai olettaa, että joku asia on itsestäänselvyys.
>
> Pelkistys: H1: Kohderyhmän ymmärtäminen ja huomioiminen

Pelkistämisen jälkeen aineisto ryhmiteltiin. Tämä tarkoittaa samankaltaisuuksien etsimistä pelkistetyistä ilmaisuista. Samaa asiaa käsittelevät näkemykset liitettiin yhteen ja niistä luotiin näkemyksiä kuvaava alaluokka. Alaluokat nimettiin niiden muodostamia näkemyksiä kuvaavalla otsikolla. (Vilkka 2021.)

Seuraavaksi esitetään esimerkki ryhmittelystä. Esimerkissä on kuuden haastateltavan litteroidun puheen pelkistysten ryhmä, joka on nimetty alaluokan otsikolla ”Tietää kenelle puhuu”:

> H1: Tietää kenelle puhuu
> H2: Kohderyhmälähtöisyys
> H3: Kohdeyleisötuntemus
> H7: Kuulijajoukko on laaja
> H9: Ymmärtää kohderyhmää
> H11: Kuulijan ymmärtäminen
>
> Alaluokka: Tietää kenelle puhuu

Seuraavaksi ryhmitellyt alaluokat käsitteellistettiin, eli ryhmittelyssä tehtyä samankaltaisuuksien etsimistä jatkettiin alaluokissa. Tämä tarkoittaa, että alaluokista muodostettiin yläluokkia, joista muodostettiin pääluokkia ja joista lopulta muodostettiin yhdistäviä luokkia. Yhdistävät luokat toimivat vastauksina tutkimuskysymyksiin. (Vilkka 2021; Tuomi & Sarajärvi 2018.) Niiden rakentuminen esitetään seuraavassa luvussa.

Käsitteellistämisen jälkeen kirjoitettiin teemahaastatteluiden analyysit. Analyyseissä esitetään yhdistävien luokkien rakenne. Tämän jälkeen analyysit lähetettiin osallistujatarkistukseen. Haastateltaville siis tarjottiin mahdollisuus tutustua tutkijan heidän haastatteluistaan tekemiin analyyseihin. Viimeisessä vaiheessa haastateltavien palaute huomioitiin ja analyysejä tarkasteltiin uudestaan niiden kautta.

5 TUTKIMUSTULOKSET

Tässä luvussa esitetään tutkimuksen tulokset, eli vastataan tutkimuskysymyksiin. Alalukujen alussa esitetään haastatteluiden keskeiset tulokset. Alaluvuissa on kuvaajia, jotka esittävät yhdistävien luokkien rakenteen. Alaluokista muodostettiin yläluokkia, joista muodostetiin pääluokkia ja joista lopulta muodostettiin yhdistäviä luokkia. Alaluokat muodostettiin haastateltavien näkemyksistä. Yhdistävät luokat selittävät ilmiötä ja vastaavat tutkimuskysymyksiin.

Tutkimustulosten esittelyn jälkeen luokkien rakennetta avataan siten, että siirrytään yhdistävistä luokista alaluokkiin. Siirtymisen aikana tuloksia havainnollistetaan aineistositaattien ja -referointien avulla. Haastatteluissa käytetty haastattelurunko löytyy liitteestä 1. Teemahaastatteluissa oli kolme teemaa: 1) kyberturvallisuuden yleistajuistaminen kansalaisille, 2) kyberturvallisuuden ymmärtämisen vastuu ja 3) kyberturvallisuuden yleistajuistamisen tarve. Vapaan sanan tulokset esitetään osana pohdintaluvun jatkotutkimusaiheita. Liitteestä 2 löytyy jokaisesta haastateltavasta kuvaus.

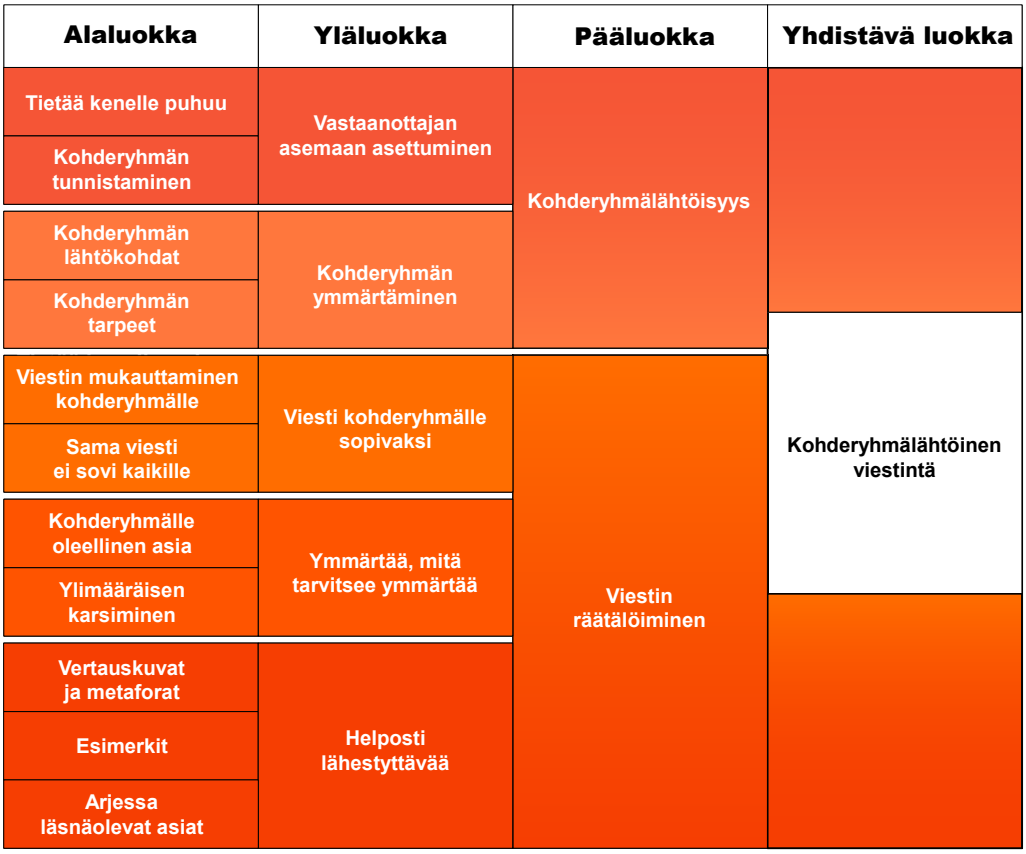
5.1 Kyberturvallisuudesta ymmärrettävämpää

Haastatteluiden perusteella kyberturvallisuuden ymmärtämisestä tehdään helpompaa kohderyhmälähtöisen viestinnän avulla ja kiinnittämällä huomiota vuorovaikutukseen ja viestin välittämiseen. Kohderyhmälähtöinen viestintä

edellyttää vastaanottajan asemaan asettumista, kohderyhmän ymmärtämistä ja viestin räätälöimistä kohderyhmälle sopivaksi. Vuorovaikutuksessa ja viestin välittämisessä korostuu asiantuntijan viestintätaidot ja erilaiset opetustavat.

Kohderyhmälähtöinen viestintä

Kuvassa 3 esitetään kohderyhmälähtöinen viestintä -yhdistävän luokan rakenne. Yhdistävä luokka jakautuu kahteen pääluokkaan: kohderyhmälähtöisyys ja viestin räätälöiminen.



Kuva 3 Kohderyhmälähtöinen viestintä -yhdistävän luokan rakenne

Kohderyhmälähtöisyys tarkoittaa asiantuntijan kykyä asettua vastaanottajan asemaan ja ymmärtää kohderyhmää. Haastatteluiden perusteella tämä on yleistajuistamisen lähtökohta. Esimerkiksi H1 totesi: *kaikki lähtee siitä, että ymmärtää sen kohderyhmän, kenelle on puhumassa*. Vastaavasti H2:n mukaan yleisön perustaso pitää ymmärtää, jotta voi viestiä ymmärrettävästi. Useat haastateltavat korostivat, että kohderyhmän tunnistaminen ja kohderyhmän lähtötason ymmärtäminen on tärkeää. Esimerkiksi H3:n mukaan kaikki lähtee siitä, että tiedostaa vastaanottavan yleisön lähtötason.

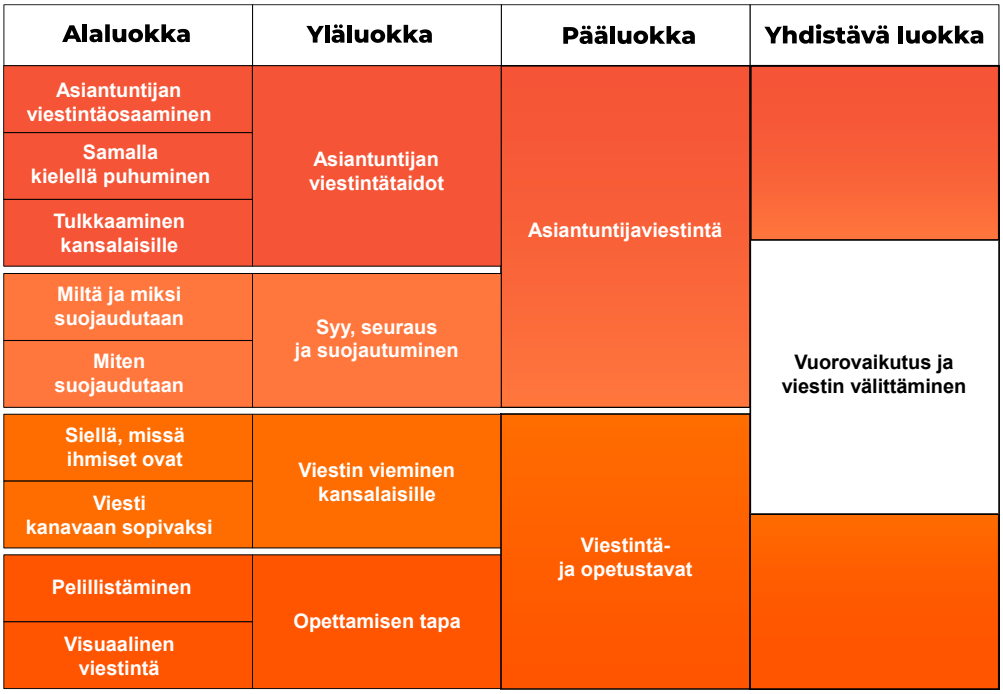
Viestin räätälöiminen tarkoittaa asiantuntijan kykyä poimia olennainen asia, muokata se kohderyhmälle sopivaksi ja tehdä käsiteltävästä asiasta helposti lähestyttävää kansalaisille. Usean haastateltavan mukaan oleellisen asian poimiminen helpottaa asian ymmärtämistä. Esimerkiksi H4:n mukaan asiantuntijan tulee kyetä hahmottamaan, mikä viestittävässä asiassa on oleellista kertoa. H5:n mukaan tulee ymmärtää, mitä kansalaisen tarvitsee ymmärtää. Asiantuntijan tulee myös mukauttaa viestintänsä kohderyhmälle sopivaksi.

Ristiriitaa vastauksissa esiintyi siinä, voiko viestiä räätälöidä kohderyhmän iän perusteella. H6 näki, että ehdottomasti, koska eri asiat koskettavat ja kiinnostavat eri ikäisiä: verkkopankkihuijaus esimerkiksi ei ole alaikäiselle ajankohtainen lainsäädännöllisistä syistä. Verkkopankkisopimuksen avaamisen alaikäraja vaihtelee pankeittain ja liikkuu 12-vuotiaasta 15-vuotiaaseen. Toisaalta esimerkiksi H9 taas ei ole valmis hyväksymään ikäperusteista yleistajuistamista. Ikäperusteinen jaottelu voi olla ongelmallista, koska osaamistaso vaihtelee ikäryhmittäin.

Haastateltavien mukaan kyberturvallisuudesta tulisi tehdä helpommin lähestyttävää. Haastatteluiden perusteella vertauskuvat, metaforat ja konkreettiset esimerkit helpottavat ymmärtämistä. Esimerkiksi H7:n mukaan kansalaiset ymmärtävät esimerkkejä helpommin kuin teknisiä yksityiskohtia. Lisäksi viestittävä asia tulee liittää kansalaisen arjessa jo läsnä oleviin asioihin. H8 sanoi: *pitää olla jollakin tavalla kytkettävissä johonkin jo älyllisesti kymmeniä vuosia sitten omaksuttuun asiaan*. H9:n mukaan ymmärtäminen on helpompaa, kun kansalainen ymmärtää, miten asia koskettaa hänen arkeaan.

Vuorovaikutus ja viestin välittäminen

Kuvassa 4 esitetään vuorovaikutus ja viestin välittäminen -yhdistävän luokan rakenne. Yhdistävä luokka jakautuu kahteen pääluokkaan: asiantuntijaviestintä sekä viestintä- ja opetustavat.



Kuva 4 Vuorovaikutus ja viestin välittäminen -yhdistävän luokan rakenne

Asiantuntijaviestintä liittyy asiantuntijan viestintäosaamiseen ja kykyyn selittää kansalaiselle, miksi ja miten asioita tehdään. Haastatteluiden perusteella ymmärrettävä viestintä on olennainen osa asiantuntijuutta. Kansalaisten kanssa ei tule esimerkiksi käyttää termejä, joita käytetään ammattilaisten kesken. H10 totesi, että asiantuntijan pitäisi pystyä keskustelemaan samalla tasolla vastaanottajan kanssa. H11 näki, että asiantuntijan tulee ymmärtää vastaanottaja ja kyetä puhumaan hänelle ymmärrettävästi. H2 totesi asiantuntijaviestinnästä: *se on sitä ammattitaitoa ja herkkyyttä, mitä vaaditaan eri toimijoilta. Se ei ole pelkästään viestinnän substanssissa työskentelevien asiantuntijoiden tehtävä, vaan entistä enemmän kaikkien asiantuntijatehtävissä toimivienkin kanssa, että miten viestisi on vaikuttavaa*.

H8:n mukaan teknologisissa murroksissa muodostuu kolme kehää. Ensimmäisellä kehällä olevat ymmärtävät murrosta, mutta eivät osaa puhua siitä ymmärrettävästi. Toisella kehällä olevat näkevät murroksen, mutta eivät ymmärrä sitä. He korvaavat ymmärtämättömyyttä kuulemiensa sanojen toistolla. Uloimmalla kolmannella kehällä on suuri väestö, kansalaiset ja koko yritysmaailma. H8:n mukaan ensimmäisen kehän asiantuntijat pitäisi tuoda kolmannelle kehälle kertomaan ymmärrettävästi murroksesta. Vastaavasti muutamassa haastattelussa puhuttiin kääntäjästä ja tulkista. Esimerkiksi H7 totesi näin: *mä en oikeastaan koe puhuvani teknologia-asioista, vaan mä oon kääntäjä. Kuten*

joku kielenkääntäjä kääntää kieleltä toiselle, mä käännän mutkikkaita teknologisia asioita sellaiselle kielelle, jota kuka tahansa ymmärtää.

Viestintätaitojen lisäksi viestinnän tyylillä on väliä. Haastatteluiden perusteella kansalaisille ei voi vain kertoa, mitä pitää tehdä. Kansalaisille pitää kertoa mitä tehdä, miksi tehdä ja konkreettisesti avata, miten toimia. Esimerkiksi H6 toteaa, että viestinnässä ei voi heti puhua ratkaisuista, vaan pitää kertoa, miksi jokin asia kannattaa tehdä. H3 painotti, että suojautumisen keinot pitää tarjota kansalaiselle konkreettisesti.

Viestintä- ja opetustavat viittaavat viestin välittämiseen kansalaisille ja erilaisiin tapoihin oppia. Haastatteluissa korostui, että viestinnässä tulee käyttää niitä kanavia, joita ihmiset käyttävät. Tämän lisäksi viesti tulee sovittaa kanavaan sopivaksi. Esimerkiksi H2:n mukaan viesti ja viestintäkanava pitää räätälöidä ajankohtaisen tiedon mukaisesti. Kolme haastateltavaa nosti esille THL:n “Oletko jo saanut kahdesti” -Tinder-koronarokotuskampanjan. Siinä viesti oli sovitettu tietyn kohderyhmän käyttämään kanavaan.

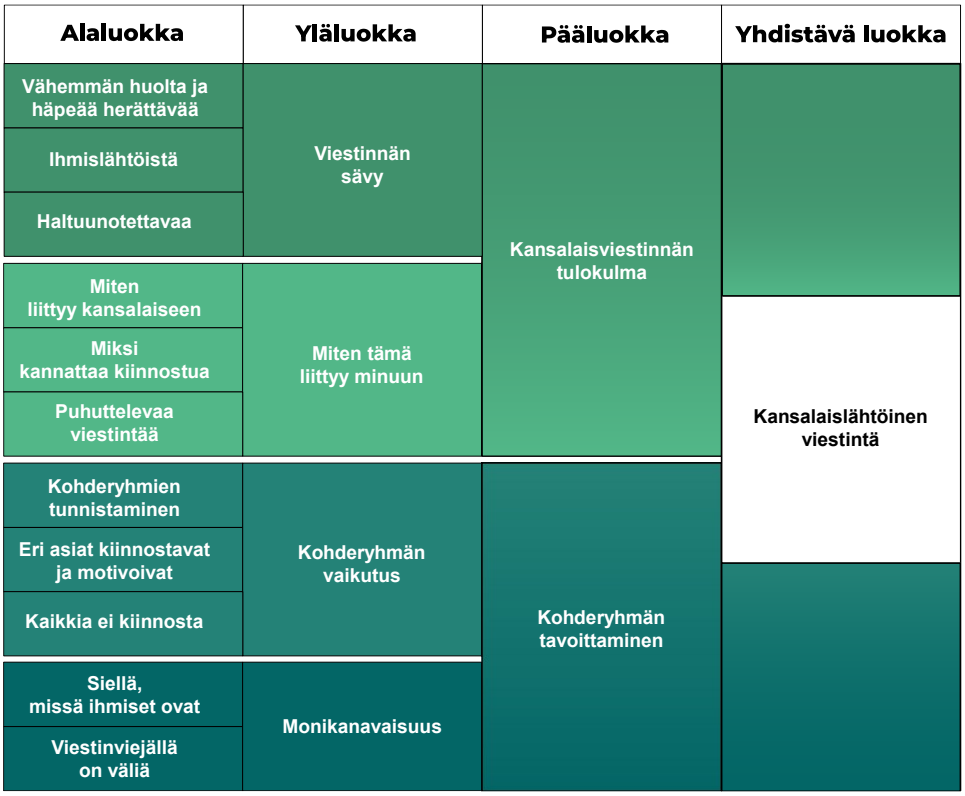
Pelillistäminen korostui opetustapana. Esimerkiksi H8:n mukaan vähitellen etenevät pelilliset elementit toimivat. Haastatteluissa todettiin, että materiaalin tulisi huomioida eri osaamistasoisia kansalaisia. Kahden haastateltavan mukaan visuaalinen viestintä lisää ymmärrettävyyttä. Opettamiseen voisi käyttää esimerkiksi kuvituksia, infografiikkaa ja lyhyitä animaatioita. H5:n mukaan ulkoa opettelu ei toimi. Sen sijaan opettamista pitäisi lähestyä taitokokonaisuuksien hallitsemisen kautta, ja kansalaisia tulisi opettaa ymmärtämään ilmiöitä.

5.2 Kyberturvallisuudesta kiinnostavampaa

Haastatteluiden perusteella kyberturvallisuudesta tehdään kiinnostavampaa kansalaislähtöisellä viestinnällä. Viestinnän tulee huomioida kansalaisten mieltymykset. Tämä edellyttää viestinnän sävyn huomioimista. Kansalaisille tulee myös kertoa, miten viestittävä asia koskettaa heitä. Lisäksi tulee huomioida erilaiset kohderyhmät ja viestiä monikanavaisesti, jotta mahdollisimman moni tavoitetaan. Ei saa myöskään unohtaa niitä, jotka eivät lähde mukaan.

Kansalaislähtöinen viestintä

Kuvassa 5 esitetään kansalaislähtöinen viestintä -yhdistävän luokan rakenne. Yhdistävä luokka jakautuu kahteen pääluokkaan: kansalaisviestinnän tulokulma ja kohderyhmän tavoittaminen.



Kuva 5 Kansalaislähtöinen viestintä -yhdistävän luokan rakenne

Kansalaisviestinnän tulokulma viittaa viestinnän sävyyn ja sen konkretisoimiseen, miten viestittävä asia liittyy kansalaiseen. Haastattelut osoittavat, että kansalaisille suunnatun viestinnän tulisi olla vähemmän huolta ja häpeää herättävää. Esimerkiksi H10:n mukaan tilanteesta tulee maalata tosiasiallinen kuva, jotta se ei herättäisi huolta. H1 totesi, että pelottelu voi johtaa lamaantumiseen. Hän lisäsi, että asia koetaan haltuunotettavammaksi, kun se on viihteellistä ja hauskaa.

Viestinnän tulee olla myös ihmislähtöistä. H5 sanoi ihmislähtöisyydestä: *tulee miettiä, onko asia oikeasti semmoinen, että ensinnäkin ihmiset voivat sen oppia järkevässä ja kohtuullisessa ajassa, ja toisekseen, että siitä oppimisesta on jotain hyötyä*. Termien käyttöön tulee myös kiinnittää huomiota. Esimerkiksi

H6:n mukaan samojen termien käyttäminen asioista auttaa säilyttämään asian tulkinnan samana, olipa esittäjä tai esittämisen kanava mikä tahansa.

Viestinnässä tulee konkretisoida, miksi asiasta kannattaa kiinnostua. Esimerkiksi H2:n mukaan asiaan ei kiinnitetä huomiota, jos kansalaiset eivät ymmärrä, miten se liittyy heidän arkeensa. H7:n mukaan kansalaisia kiinnostaa vain silloin, kun he ovat joutuneet hyökkäyksen kohteeksi tai kokeneet läheltä piti -tilanteen. Haastatteluiden perusteella kyberturvallisuus tulisi linkittää osaksi kansalaisten arkea. Esimerkiksi H9:n mukaan kansalaisia tavoitetaan paremmin, kun koulutus ja viestintä liitetään yhteiskunnalliseen toimintaan, kuten oppilaitoksiin ja työpaikoille. Vastaavasti H10:n mukaan tieto pitää tuoda silmien eteen, koska sitä ei aktiivisesti etsitä, jos siitä ei olla kiinnostuneita.

Kohderyhmän tavoittaminen tarkoittaa monikanavaista viestintää ja kohderyhmän huomioimista. Kohderyhmän tunnistaminen ja ymmärtäminen ovat avainasemassa. On vaikea lisätä kiinnostusta, jos kohderyhmän kiinnostuksen kohteita ei tiedetä. Esimerkiksi H5:n mukaan kansalaisilla on erilaiset kiinnostuksen kohteet ja H11:n mukaan eri asiat motivoivat eri ihmisiä. H6:n mukaan pitää ymmärtää kohderyhmän taustatiedot, ennen kuin voidaan miettiä, miten kiinnostusta lisätään.

Haastatteluiden perusteella pitää käyttää niitä kanavia, joita kansalaiset käyttävät. H2:n mukaan ihmisten huomiosta joudutaan kilpailemaan päivittäisessä viestitulvassa. H5:n mukaan viestintää pitää tehdä pitkäjänteisesti, suunnitelmallisesti ja eri kanavissa. H3 totesi, että viestintää tulee tehdä monikanavaisesti kohdeyleisö tuntien. Viestinviejällä on haastatteluiden mukaan myös merkitystä; esimerkiksi vastaanottajan kulttuurisen taustan takia viranomaiseen ei välttämättä luoteta.

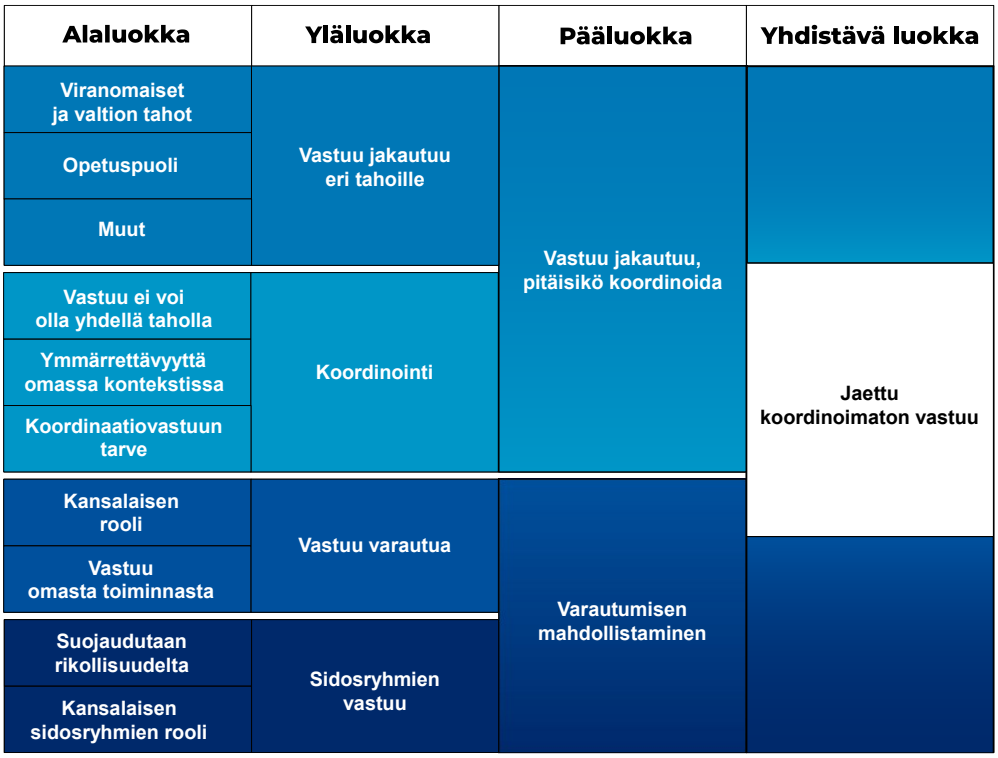
Haastatteluissa korostetaan, että kaikkia kansalaisia ei saada kiinnostumaan kyberturvallisuudesta. Kansalaisia ei voida myöskään pakottaa kiinnostumaan. Esimerkiksi H10:n mukaan sataprosenttista kattavuutta ei tulla saavuttamaan, mutta mahdollisimman suuri on riittävä. H8:n mukaan ei saa kuitenkaan unohtaa niitä, jotka eivät halua tai kykene lähtemään mukaan.

5.3 Kyberturvallisuuden ymmärtämisen vastuu

Haastatteluiden perusteella näyttää siltä, että kyberturvallisuuden ymmärtämisen vastuu on jaettua ja koordinoimatonta. Tulosten perusteella ei määritellä virallisia vastuutahoja, vaan kuvataan, miten haastateltavat näkivät tilanteen. Haastateltavien mukaan yksittäinen taho ei vastaa siitä, että kansalaiset ymmärtävät kyberturvallisuutta. Vastuu jakautuu eri toimijoille. Kansalaisten nähtiin erityisesti vastaavan omasta toiminnastaan ja varautumisestaan digitaalisessa maailmassa.

Jaettu koordinoimaton vastuu

Kuvassa 6 esitetään jaettu koordinoimaton vastuu -yhdistävän luokan rakenne. Yhdistävä luokka jakautuu kahteen pääluokkaan: vastuu jakautuu, pitäisikö koordinoida ja varautumisen mahdollistaminen.



Kuva 6 Jaettu koordinoimaton vastuu -yhdistävän luokan rakenne

Vastuu jakautuu, pitäisikö koordinoida tarkoittaa, että vastuu jakautuu usealle eri toimijalle. Lisäksi haastatteluissa pohdittiin koordinoinnin tarvetta. Haastateltavien mukaan viranomaisilla, valtion tahoilla ja opetuspuolella on vastuuta. Viranomaisista ja valtion tahoista mainittiin Kyberturvallisuuskeskus,

Traficom, poliisi, Keskusrikospoliisi, Maanpuolustuskoulutusyhdistys, Digi- ja väestötietovirasto ja Vanhustyön keskusliitto. Myös opetuspuolella nähtiin selkeästi vastuuta. Esimerkiksi H4:n mukaan opetuspuolella on sisältöjä ja pedagogista osaamista levittää tietoisuutta yhteiskunnassa. Näiden lisäksi muutamissa haastatteluissa vastuuta jaettiin asiantuntijoille, työnantajille, vanhemmille ja medialle. Haastateltavat näkivät myös, että eri toimijoiden vastuulla olisi lisätä ymmärrystä omassa kontekstissaan.

Jaettu vastuu herättää tarpeen harkita koordinoinnin lisäämistä vastuukenttään. Esimerkiksi H4 totesi, että yksittäisen tahon on haastavaa vastata siitä, että suomalaiset tietävät, mitä kyberturvallisuus tarkoittaa. H5:n mukaan ei pitäisi tuoda lisää toimijoita mukaan, vaan tulisi miettiä, miten nykyisen kokonaisuuden saisi toimimaan paremmin. H10 nosti esille, että hajautetun vastuun takia yhden toimijan ääni ei välttämättä nouse tarpeeksi.

Varautumisen mahdollistaminen viittaa siihen, että kansalaisella nähtiin olevan vastuu varautua uhkiin – tämä pitäisi kuitenkin mahdollistaa. Monen haastateltavan mukaan kansalaisilla on vastuu huolehtia ymmärtämisestä pääsääntöisesti itse. Kyberturvallisuuden nähtiin siis kuuluvan kaikille. Esimerkiksi H7:n mukaan päävastuu on kansalaisella itsellään, koska heidän datansa ja rahansa ovat pelissä. H9 totesi, että kansalainen voi olla toimenpiteen kohde, mutta myös aktiivinen toimija, ja tällöin omat oikeudet ja vastuut pitää tietää.

Haastatteluiden perusteella kansalaisilla on vastuu omasta toiminnastaan. H5 totesi, että digitaalisen maailman säännöt pitää tietää ja niitä tulee noudattaa. Vastaavasti H4:n mukaan kansalaisen pitää tietää, miten digitaalisessa maailmassa toimitaan. Kansalaisten vastuu näyttäisi kohdistuvan omaan toimintaan digitaalisessa maailmassa. Tämän lisäksi nähtiin, että kansalaisten tulisi aktiivisesti varautua uhkiin. H3:n mielestä kansalaisella on vastuu omasta varautumisestaan: *se ei ole mun mielestä ehkä vastuu siitä, että kuka sen ymmärtää, vaan sulla on vastuu huolehtia siitä omasta varautumisesta*.

Muutama haastateltava huomautti, että kansalaiset suojautuvat rikollisilta, ja sen takia vastuun rajoja pitää miettiä. H2:n mukaan kyberturvallisuus on kokonaisuus, joka muodostuu muun muassa rikosten ennaltaehkäisystä ja torjunnasta. Vastuu yhteiskunnassa on jaettua ja sen takia toimijoiden tulee miettiä

oman roolinsa ja tehtäviensä kautta, miten ihmisten tietotaitoa ja osaamista ylläpidetään ja tuetaan. Vastaavasti H1 totesi: *mun mielestä tässä on hyvä punnita, missä kohtaa menee meidän vastuu suojella ihmisiä ja estää rikollisuutta, ja missä menee heidän vastuu siinä, mitä pitäisi edes osata ymmärtää*.

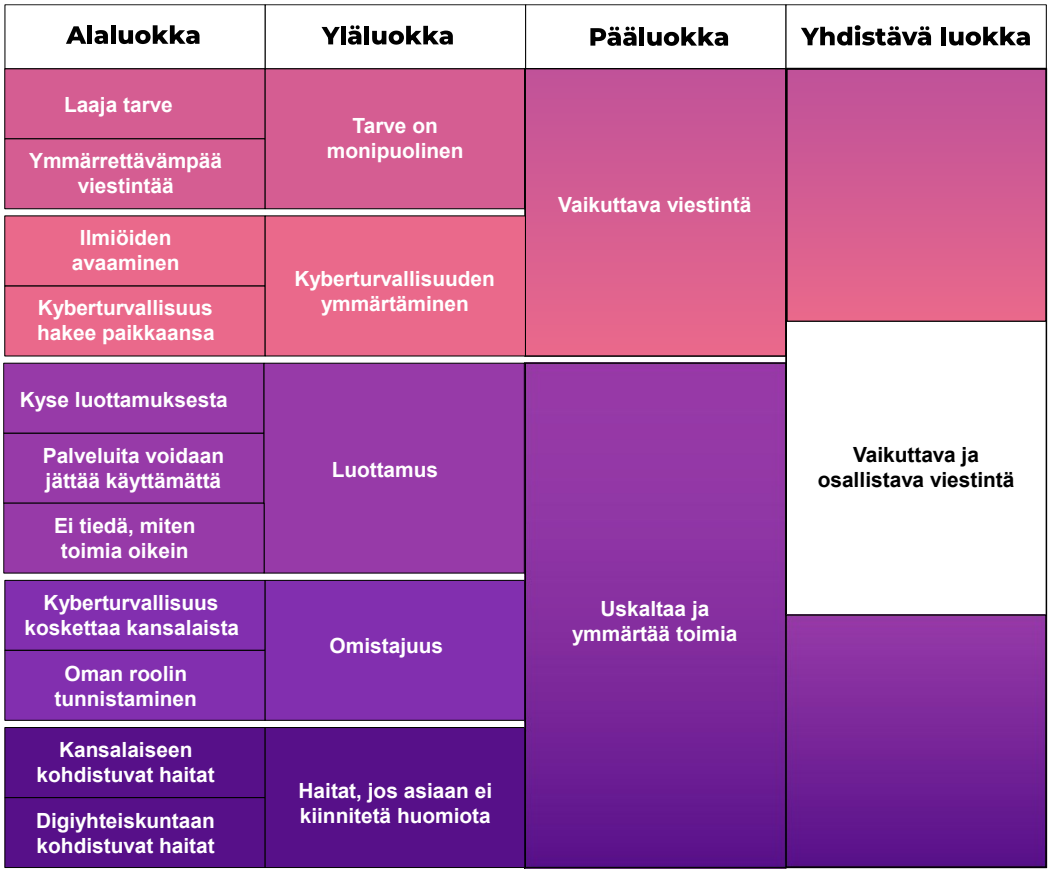
Muutama haastateltava keskusteli kansalaisten sidosryhmien vastuusta. Esimerkiksi H5 korosti kansalaisen oman vastuun rinnalla sitä, että kansalaisille pitää tarjota keinoja omien vastuiden tunnistamiseen ja tarvittavien taitojen oppimiseen. Vastaavasti H1:n mukaan vastuu kuulostaa siltä, että uhri kantaa vastuun, vaikka uhrin olisi hyvä saada tietää esimerkiksi minkälaisia oikeuksia hänellä on ja mistä hän voi pyytää apua.

5.4 Kyberturvallisuuden yleistajuistamisen tarve

Haastatteluiden perusteella vaikuttavalle ja osallistavalle viestinnälle on tarvetta. Viestinnän tulee olla ymmärrettävää, jotta kansalaiset voivat omaksua kyberturvallisuutta ja tunnistaa roolinsa siinä. Epäselvä viestintä voi heikentää luottamusta ja johtaa siihen, ettei palveluita käytetä. Haastatteluiden perusteella jatkuvasti kehittyvä ja kohdennettu viestintä on haaste. Teknologian ja uhkakuvien nopea kehitys luo ennalta-arvaamattomuutta. Kyberturvallisuuden monimutkaisuus ja resurssien rajallisuus haastavat yleistajuistamista. Lisäksi viestinnältä edellytetään kykyä mukautua eri kohderyhmien tarpeisiin.

Vaikuttava ja osallistava viestintä

Kuvassa 7 esitetään vaikuttava ja osallistava viestintä -yhdistävän luokan rakenne. Yhdistävä luokka jakautuu kahteen pääluokkaan: vaikuttava viestintä ja uskaltaa ja ymmärtää toimia.



Kuva 7 Vaikuttava ja osallistava viestintä -yhdistävän luokan rakenne

Vaikuttava viestintä tarkoittaa, että yleistajuistamiselle on monipuolinen tarve. Esimerkiksi H7:n mukaan kansalaiset eivät ymmärrä isoa osaa kyberturvallisuusalan keskustelusta. H4 totesi: *tarve tulee siitä, että se on nykyään osa kaikkien kansalaisten arkea, eli kyllä se osaaminen on saatava samalla tavalla sen arjen osaksi kuin ne digitaaliset teknologiat ja palvelut*. Vastaavasti H8:n mukaan tarvetta on, koska kyberturvallisuus on osa arkista yhteiskuntaa. Vastaavasti H11 korosti, että digitalisaation takia kyberturvallisuus on nykypäivänä tarvittava taito.

Haastatteluiden perusteella ymmärrettävä viestintä vaikuttaa siihen, millainen kuva kyberturvallisuudesta välittyy kansalaisille. Esimerkiksi H1:n mukaan tilanteiden taustalla olevat syyt pitää avata ymmärrettävästi, koska se poistaa mystiikkaa kaikkivoipaisista rikollisista. Lisäksi nähtiin, että kyberturvallisuus hakee paikkaansa. Esimerkiksi H7:n mukaan alussa kyberturvallisuudella ei ollut kansalaisille merkitystä, koska he eivät käyttäneet tietoverkkoja lainkaan. Murroksen myötä kyberturvallisuudesta on tullut kansalaisille yhä tärkeämpää.

Uskaltaa ja ymmärtää toimia viittaa luottamukseen, omistajuuteen ja haittoihin, joita voi syntyä, jos yleistajuistamiseen ei kiinnitetä huomiota. Haastatteluiden perusteella luottamus heikentyy, jos viestintä on epäselvää. Tämä voi johtaa siihen, että palveluita jätetään käyttämättä. Esimerkiksi H2:n mukaan viestinnän tärkeä tehtävä on auttaa ihmisiä pysymään kehityksessä mukana. H3 tarkensi, ettei kyse välttämättä ole epäluottamuksesta, vaan epävarmuudesta. Vaikeaselkoiset viestit voivat myös aiheuttaa väärinkäsityksiä.

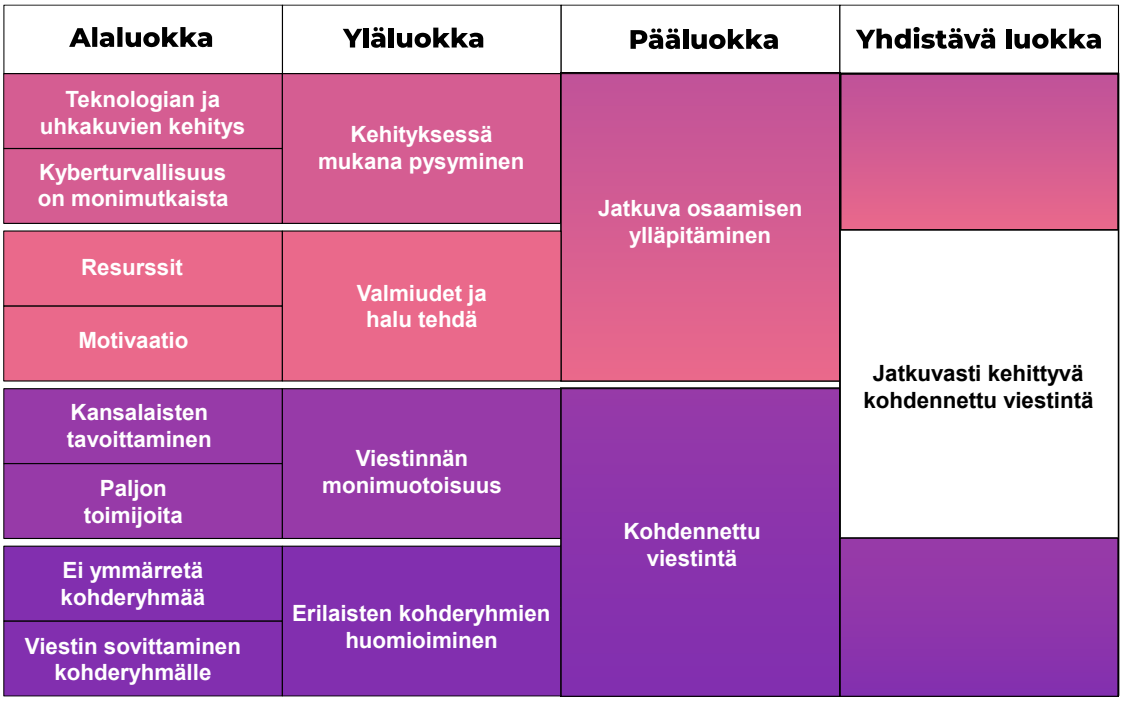
Yleistajuistaminen vaikuttaa myös omistajuuteen, eli oman roolin tunnistamiseen. Esimerkiksi H8:n mukaan kansalaisten pitää ymmärtää oma osuutensa. H1:n mukaan tulee puhua ymmärrettävästi, jotta kansalaiset kokevat asian kuuluvan heille. Lisäksi pitää perustella, miksi kansalaiset välittäisivät omasta kyberturvallisuudesta. H5 totesi, että ihmisillä on paljon kaikkea ja sen takia syyn löytäminen on haastavaa.

Haittoja voi syntyä, jos yleistajuistamiseen ei kiinnitetä huomiota. Kansalaiseen kohdistuvat haitat liittyivät erityisesti taloudellisiin menetyksiin ja heikentyvään tietotaitoon. H5:n mukaan tietotaidon heikentymisen takia kansalaiset ovat alttiimpia rikoksille. H6:n mukaan voi muodostua ryhmiä, jotka suhtautuvat kyberturvallisuuteen negatiivisesti ja sivuuttavat aiheeseen liittyvän viestinnän kokonaan, jollei itse viestintää olla toteutettu kyseisen ryhmän tietotaitotason mukaiseksi.

Digitaalinen yhteiskunta voi myös muuttua haavoittuvammaksi kansalaisten osaamistason heikentymisen takia. H7 luetteli haittoja: *verkkorikollisuus kasvaa. Yksityisyyden loukkaukset kasvaa. Tietovuodot kasvaa. Haittaohjelmaepidemiat kasvaa ja rikollisorganisaatiosta tulee yhä voimakkaampia ja rikkaampia. Ja tää ongelma vaan kiihtyy ja mennään yhä enemmän semmoista tilannetta kohti, missä netti on laiton alue eli siellä on säännöt kuin villissä lännessä. Rikoksia voi tehdä vapaasti, koska niistä ei koskaan jää kiinni ja jos jää kiinni niin tuomiot ovat mitättömiä*.

Jatkuvasti kehittyvä ja kohdennettu viestintä

Kuvassa 8 esitetään jatkuvasti kehittyvä kohdennettu viestintä -yhdistävän luokan rakenne. Yhdistävä luokka jakautuu kahteen pääluokkaan: jatkuva osaamisen ylläpitäminen ja kohdennettu viestintä.



Kuva 8 Jatkuvasti kehittyvä kohdennettu viestintä -yhdistävän luokan rakenne

Jatkuva osaamisen ylläpitäminen on haaste, koska viestinnässä on pysyttävä kehityksen mukana. Esimerkiksi H2:n mukaan toimintaympäristö muuttuu jatkuvasti, minkä takia mukana pysyminen on haastavaa. Teknologian ja uhkakuvien nopea kehittyminen tekee kyberturvallisuusalasta ennalta-arvaamatonta. Välillä pitää päiväkohtaisesti miettiä, miten asioista viestitään kansalaisille. Tekoäly vaikeuttaa tilannetta entisestään. Kyberturvallisuus on myös monimutkaista. Esimerkiksi H7 totesi, että selittäminen muuttuu vaikeammaksi, koska uusia teknologioita luodaan vanhojen päälle. H5 totesi, että ammattilaisillakaan ei ole yhdenmukaista käsitystä siitä, mitä kyberturvallisuus on.

Haasteena on myös resurssit ja motivaatio. Resurssit viittaavat siihen, kuka kustantaa yleistajuistamisen. Esimerkiksi H5 pohti, pitääkö ihmisten itse maksaa siitä, että he ovat valveutuneita kyberturvallisuusasioissa. H8 totesi ihmisten kehistä, että on työlästä löytää ensimmäisen kehän tahot ja tuoda heidät

popularisoivalla mekanismilla kolmannelle kehälle. Vastaan voi tulla myös motivaatio. Esimerkiksi H4 totesi, että korkeakoulujen resursoinnissa heijastuu asenne, jossa kansanvalistukseen ei ole hirveästi pyrkimystä. Tämä johtuu siitä, että se ei hyödytä korkeakouluja, eikä se välttämättä edistä asiantuntijoiden urakehitystä.

Kohdennettu ja monipuolinen viestintä on haaste, koska viestinnän tulee huomioida erilaisia kohderyhmiä. Haastatteluiden perusteella kansalaisten tavoittaminen voi olla monimutkaista, sillä tietoa ja toimijoita on paljon. Kaikkia kansalaisia ei ikinä tavoiteta. Esimerkiksi H3 totesi, että kokonaisviestin julistaminen on vaikeaa ja se haastaa ymmärryksen lisäämistä. Toisaalta H2:n mukaan haasteena on toimijoiden oman ammattitaidon ylläpitäminen.

Haasteena on myös kohderyhmien erityistarpeiden huomioiminen. Esimerkiksi H2 huomautti, että Suomessa asuu entistä enemmän ihmisiä, joiden äidinkieli ei ole suomi tai ruotsi. Vastaavasti H4:n mukaan yleistajuistamista katsotaan yleensä suomalaisen suomea puhuvan henkilön näkökulmasta. Haastatteluissa korostettiin myös psyykkisiä ja fyysisiä rajoitteita. H5 huomautti, että erityisesti näiden kohderyhmien tarpeita huomioidaan huonosti tällä hetkellä. Esimerkiksi tietojen kalastelun tunnistamista opetetaan näkevän ihmisen näkökulmasta. Viestin sovittaminen kohderyhmälle asettaa myös painetta viestinnälle.

5.5 Yhteenveto

Kyberturvallisuudesta ymmärrettävämpää -alaluvussa kuvattiin, miten haastateltavien mukaan kyberturvallisuudesta voidaan tehdä ymmärrettävämpää kansalaisille. Tulosten perusteella asiantuntijan on ymmärrettävä kohderyhmän lähtötaso ja tarpeet, jotta viestintä voidaan räätälöidä heille sopivaksi. Oleellisen asian poimiminen tekee viestistä ymmärrettävämmän. Lisäksi viestin ymmärrettävyyttä edistää vertauskuvien, metaforien ja esimerkkien käyttö, ja käsiteltävän asian liittäminen kansalaisen arjessa oleviin asioihin.

Asiantuntijan pitää pystyä viestimään tavalla, jonka vastaanottaja ymmärtää. Teknologisissa murroksissa esiintyy kolme kehää, joille ihmiset sijoittuvat. Asiantuntijoiden tehtävänä on viedä ymmärrettävästi tietoa ensimmäiseltä kehältä kolmannelle kehälle, eli kansalaisille. Viestinnässä on olennaista selittää,

miksi asia kannattaa tehdä, ja tarjota konkreettisia toimintaohjeita. Pelkkä kehotus tekemiseen ilman perusteluita ei riitä. Pelillistämisen ja visuaalisen viestinnän nähtiin lisäävän ymmärrettävyyttä.

Kyberturvallisuudesta kiinnostavampaa -alaluvussa kuvattiin, miten haastateltavien mukaan kyberturvallisuudesta voidaan tehdä kiinnostavampaa kansalaisille. Tulosten perusteella viestinnän tulisi olla ihmislähtöistä ja vähemmän huolta ja häpeää herättävää. Tärkeää on konkretisoida, miten kyberturvallisuus liittyy kansalaisten arkeen ja miksi heidän kannattaa kiinnostua aiheesta. Kohderyhmän ymmärtäminen on olennaista, ja viestintää tulee tehdä niissä kanavissa, joissa kansalaiset ovat. Lopulta kaikkia ei kuitenkaan saada kiinnostumaan. Siksi on tärkeää muistaa myös ne, jotka eivät ole kiinnostuneita tai kykene osallistumaan.

Kyberturvallisuuden ymmärtämisen vastuu -alaluvussa kuvattiin, keiden vastuulla on varmistaa, että kansalaiset ymmärtävät kyberturvallisuutta. Tulosten perusteella vastuu jakautuu eri toimijoiden kesken – viranomaisilla, valtion tahoilla ja opetussektorilla nähdään selkeä vastuu. Jaettu vastuunjako herätti keskustelua koordinaation tarpeesta. Kansalaisten nähtiin olevan vastuussa omasta toiminnasta ja varautumisesta. Toisaalta kyberturvallisuus liittyy rikollisuuden torjuntaan, joten kansalaisten vastuun rajat vaativat harkintaa. Kansalaisille tulisi myös tarjota tukea, jotta he voivat suoriutua roolistaan.

Kyberturvallisuuden yleistajuistamisen tarve -alaluvussa kuvattiin, millainen tarve haastateltavien mukaan kyberturvallisuuden yleistajuistamiselle on. Tulosten perusteella yleistajuistamiselle on monipuolinen tarve. Epäselvä viestintä voi johtaa luottamuksen heikkenemiseen ja palveluiden välttämiseen. Ymmärrettävä viestintä vahvistaa luottamuksen lisäksi omistajuutta, eli sitä, että kansalaiset ymmärtävät ja omaksuvat roolinsa kyberturvallisuudessa.

Yleistajuistamisen keskeiset haasteet ovat teknologian ja uhkakuvien nopea kehitys ja kyberturvallisuuden monimutkaisuus. Näiden takia asiantuntijoiden on jatkuvasti pysyttävä ajan tasalla. Yleistajuistamista haastaa myös resurssit ja motivaatio: minkä takia yleistajuistamista tehtäisi ja kuka tekemisen maksaa? Lisäksi kohderyhmien erityistarpeiden huomioiminen on haaste. Esimerkiksi kielellisiä, psyykkisiä ja fyysisiä rajoitteita tulisi huomioida paremmin.

6 JOHTOPÄÄTÖKSET

Tässä luvussa esitetään tutkimuksen johtopäätökset, eli vastataan tutkimusongelmaan. Tutkimuksen tutkimusongelma on: *kyberturvallisuus koskettaa jokaista meistä, ja sen takia sen pitäisi olla myös ymmärrettävää jokaiselle meistä. Tämän takia ymmärrettävämpään kyberturvallisuusviestintään olisi syytä kiinnittää enemmän huomiota.* Tavoitteena oli siis selvittää, miten kyberturvallisuudesta voidaan viestiä ymmärrettävämmin kansalaisille.

Kaikki lähtee kohderyhmästä

Tämän tutkimuksen teemahaastatteluiden perusteella näyttää siltä, että kyberturvallisuuden yleistajuistamisessa kaikki lähtee kohderyhmästä. Yleistajuistajan tulisi kyetä ajattelemaan kuten viestinnän kohderyhmä ja tarkastella aihetta heidän näkökulmastaan. Aiheen tarkastelu kohderyhmän näkökulmasta on oleellista siksi, että kohderyhmät ovat erilaisia. Esimerkiksi kohderyhmän tietotaitotaso, tarpeet ja kiinnostuksen kohteet voivat vaihdella. Kohderyhmänä voi olla jopa yksittäinen kansalainen. Kansalaisten lähestyminen yhtenä massana samanlaisella viestillä ei näytä toimivan.

Kyberturvallisuuden ymmärtämistä näyttää helpottavan se, miten hyvin viesti puhuttelee vastaanottajaa. Yleistajuistajan on kyettävä luomaan yhteys vastaanottajan kokemusmaailmaan. Kohderyhmä näyttää ohjaavan myös niitä valintoja, joita yleistajuistamisessa tehdään esimerkiksi viestin sisällön, esittämistavan ja viestintäkanavan suhteen.

Tutkimus antaa viitteitä siitä, että ymmärrettävyys ei yksin riitä, jos halutaan lisätä kansalaisten kyberturvallisuusosaamista. Kyberturvallisuuteen ja sen viestintään ei välttämättä kiinnitetä huomiota, jos kansalainen ei koe sitä merkitykselliseksi. Ymmärrettäväkin viestintä saatetaan sivuuttaa, jos se ei ole kiinnostavaa tai siitä ei ole hyötyä kansalaiselle. Kohderyhmä ohjaa siis yleistajuistajan valintoja jatkuvasti viestinnän suunnittelusta sen toteutukseen.

Kyberturvallisuuden tulkki

Kyberturvallisuus on monimutkaista. Näyttää siltä, että monimutkaisuuden takia kyberturvallisuuden ja kansalaisen väliin tarvitaan tulkkeja. Kyberturvallisuuden tulkki yleistajuistaa kyberturvallisuutta kansalaiselle ymmärrettävään muotoon. Yleistajuistamista tehdessä olisi hyvä ottaa seuraavat kysymykset huomioon: 1) mitä, 2) miksi, 3) missä ja 4) miten viestitään?

Mitä kyberturvallisuudesta viestitään tarkoittaa viestinnän sisältöä. Yleistajuistamisessa olisi hyvä miettiä, mitä tietoa kohderyhmälle halutaan välittää. Mikä on se ilmiö, josta kohderyhmän pitäisi tietää lisää. Tämä voi liittyä esimerkiksi uhkiin tai suojautumistoimiin, joita kansalaisen olisi hyödyllistä ymmärtää. Tulkki toimii tässä tiedon suodattajana ja välittää kohderyhmälle vain olennaisen tiedon ilmiöstä.

Miksi kyberturvallisuudesta viestitään tarkoittaa viestinnän tavoitetta. Yleistajuistamisessa olisi hyvä miettiä, miksi juuri tämä tieto halutaan välittää kohderyhmälle. Mitä viestinnällä halutaan saavuttaa, ja onko tiedosta ylipäätään hyötyä kansalaiselle? Viestin tavoite näyttää vaikuttavan siihen, miten merkittäväksi kansalaiset kokevat viestittävän asian. Tulkin tehtävä on konkretisoida kansalaisille, miksi viestittävästä asiasta kannattaisi tietää lisää.

Missä kyberturvallisuudesta viestitään tarkoittaa viestinnän kanavaa. Yleistajuistamisessa olisi hyvä miettiä, missä kanavassa viesti välitetään. Kanava riippuu kohderyhmästä. Tavoitteena on saavuttaa kansalaiset siellä, missä he ovat aktiivisia ja vastaanottavaisia viesteille. Tulkin tulee valita viestintäkanavat, jotka tavoittavat kansalaiset heidän arjessaan.

Miten kyberturvallisuudesta viestitään tarkoittaa viestinnän tyyliä. Yleistajuistamisessa tulee miettiä, miten viesti esitetään kohderyhmälle. Viestinnän tulisi olla ymmärrettävää ja helposti lähestyttävää. Viestin tyyli pitää sovittaa kohderyhmän, tavoitteen ja viestintäkanavan mukaiseksi. Tulkin tehtävä on räätälöidä viestintä kohderyhmälle sopivaksi.

Kansalaisen omistajuuden ja vastuun korostaminen

Tämän tutkimuksen perusteella kansalaisten omistajuutta kyberturvallisuudessa olisi hyvä lisätä. Vaikka tämä ei suoranaisesti liity ymmärrettävään viestintään, voisi sen ehkä ajatella liittyvän viestin ymmärtämiseen. Mitä enemmän kansalaiset aktiivisesti hoitavat omaa rooliaan kyberturvallisuudessa, sitä syvemmin he perehtyvät kyberturvallisuuteen liittyvään tietoon. Yhteiskunnan kyberturvallisuus rakentuu yhteistyöllä, jossa myös kansalaisilla on oma roolinsa. Tähän voisi viitata myös se, että kyberturvallisuus nähdään nykypäivän kansalaistaitona (luku 3.5). Kansalaiset olisi siis hyvä saada ymmärtämään oma roolinsa ja aktiivisesti toimimaan sen mukaan. Vaikka tarve omistajuudelle on tunnistettu, vastuun jakautumista ei selvitetty yksiselitteisesti tutkimuksessa. Esiin nousi kuitenkin tarve miettiä, missä menee kansalaisten vastuu, ja missä sidosryhmien vastuu kansalaisesta.

Tutkimus antaa viitteitä siitä, että kansalaisten omistajuuden ja vastuun korostaminen voisi edistää ymmärrystä ja osallistumista kyberturvallisuuteen. Tällä tavalla viestinnässä itsessään olisi jo mukana perustelut sille, miksi asiasta kannattaa kiinnostua. On kuitenkin huomioitava, että kansalaisten vastuun tulee olla yhteisesti määriteltyä, jotta siitä voidaan viestiä ymmärrettävästi.

Yleistajuistaminen pitää mahdollistaa

Tämä tutkimus havainnollistaa, että asiantuntijoiden ja kansalaisten osaamistason kehittämisen pitää olla jatkuvaa. Tämä johtuu siitä, että teknologian ja uhkakuvien kehitys on jatkuvaa. Yleistajuistamista on siis tehtävä jatkuvasti, jotta kansalaiset voivat pysyä kehityksen mukana. Tämä edellyttää, että yleistajuistamisen tekeminen mahdollistetaan.

Kyberturvallisuuden ymmärtämiseen voi vaikuttaa se, kuinka paljon siihen ohjataan resursseja. Kysymys on siitä, kuka yleistajuistamista tekee ja millä voimavaroilla. Yleistajuistamisen tekeminen ei ole välttämättä mielekästä, jos se ei vaikuta myönteisesti esimerkiksi asiantuntijan urakehitykseen tai taloudelliseen tilanteeseen. Asiantuntijoista ei voi myöskään tulla kyberturvallisuuden tulkkeja, jos heillä ei ole mahdollisuutta kehittää osaamistaan siinä.

Yleistajuistamiseen olisi siis olennaista kannustaa ja siitä pitäisi tehdä houkuttelevaa. Kyberturvallisuuden tulkkeja tarvitaan, joten heidän motivoimisensa on keskeistä. Tämän takia resurssointiin ja motivointiin olisi hyvä kiinnittää jatkossa enemmän huomiota. Kyse voi olla jopa kansalaisten luottamuksesta; luottamus voi heikentyä, jos viestintä on liian vaikeaa tai epäselvää.

7 POHDINTA

Tässä luvussa esitetään tutkimuksen pohdinta. Luvussa käsitellään, miten tutkimus toteutui, tarkastellaan sen luotettavuutta ja verrataan tutkimuksen tuloksia teoreettiseen viitekehykseen. Lisäksi kuvataan jatkotutkimusaiheet.

Tutkimus toteutui tutkimussuunnitelman ja aikataulun mukaan monimenetelmällisyyttä lukuun ottamatta. Tutkimuksessa siirryttiin yhden vaiheen jälkeen seuraavaan siten, että ennen siirtymistä tutustuttiin seuraavaan vaiheeseen ja tarvittaessa haettiin tukea siihen. Opinnäytetyön tekeminen oli tutkijalle uusi asia, ja se osaltaan aiheutti haasteita. Erityisesti uuden aihealueen, kyberturvallisuuden viestinnän, ja tutkimusmenetelmien omaksuminen vaati aikaa. Teoreettisessa viitekehyksessä on tämän takia puutteita: viestinnän ilmiöitä ja kyberturvallisuuden viestinnän aiempia tutkimuksia olisi pitänyt selvittää laajemmin. Puutteitta ei perustella sillä, ettei sopivia tutkimuksia olisi ollut, koska tutkija on kokematon aineiston etsimisessä.

Teemahaastattelut olivat merkittävä osa tutkimusta. Niihin valmistauduttiin hyvin, jotta niistä saatava aineisto olisi laadukasta. Ennen haastatteluita varmistettiin, että haastateltavat tietävät oikeuksistaan ja osallistumisen vapaaehtoisuudesta. Heille lähetettiin myös haastattelun kysymysrunko (liite 1), jotta he voisivat valmistautua kysymyksiin etukäteen. Ennen varsinaisia haastatteluita pidettiin myös kolme harjoitushaastattelua. Harjoitushaastatteluiden avulla tutkija harjoitteli haastattelijana oloa ja testasi kysymyksiä.

Haastattelijana toimiminen muuttui luontevammaksi harjoitushaastatteluiden jälkeen. Haastattelut toteutuivat kokonaisuutena hyvin. Huomioitava puute oli kuitenkin haastatteluiden ajanhallinta. Haastattelut kestivät keskimäärin 45 minuuttia, joista kolme 60 minuuttia ja yksi 30 minuuttia. Muutamissa haastatteluissa loppua kohti joutui kiihdyttämään, jotta kaikki teemat ehdittiin käsitellä.

Tämä johtui tutkijan haastattelutaidoista. Pieni nopeutus ei kuitenkaan ollut merkittävää, koska kaikki teemat ehdittiin käydä kaikkien kanssa läpi. Lisäksi ensimmäinen teema oli tutkimuksen kannalta tärkein.

Tutkimuksen aiheen takia tutkimuksen raportin ymmärrettävyyteen ja selkeyteen panostettiin. Tutkija kiinnitti huomiota ymmärrettävään kieleen, selkeisiin lauserakenteisiin ja johdonmukaiseen kappalerakenteeseen, jota selkeytettiin alaotsikoiden avulla. Tekstissä hyödynnettiin visualisointeja ja yhteenvetojen avulla poimittiin oleellinen asia laajemmasta tekstimassasta. Kokonaisuudesta haluttiin helposti lähestyttävä ja ymmärrettävä.

Luotettavuustarkastelu

Seuraavaksi palataan luotettavuusvaraumassa asetettuihin tutkimuksen luotettavuuden arvioimisen tapoihin. Keskeisessä roolissa oli tutkijan luotettavuus, eli tutkijan tekemät valinnat, ratkaisut ja teot. Läpinäkyvyys ohjasi tutkimuksen tekemistä. Tämä näkyi esimerkiksi siinä, että tutkimuksen eri vaiheet tallennettiin. Tämä tarjosi mahdollisuuden palata analyysivaiheita taaksepäin ja varmistaa tulosten oikeellisuus. Tutkija tavoitteli laadukasta lopputulosta ja se näkyi suunnitelmallisessa toiminnassa.

Tuen hakeminen oli olennainen osa tutkimuksen tekemistä. Palautetta ja erilaisia näkemyksiä haettiin, jotta tutkimuksen lopputuloksesta tulisi laadukkaampi. Tukea haettiin aktiivisesti tutkimuksen eri vaiheissa. Palautteen avulla tunnistettiin esimerkiksi, että tutkijan tekemien valintojen perustelemiseen ja avaamiseen tulisi kiinnittää enemmän huomiota. Saatu palaute otettiin huomioon ja tutkimusta parannettiin palautteiden avulla.

Tutkimuksen validiteettiin kiinnitettiin erityistä huomiota. Tutkimusmenetelmät valittiin huolellisesti, jotta tutkittavaa ilmiötä tutkitaan oikealla tavalla. Aineistolähtöisen sisällönanalyysin vaiheet kuvattiin (luvut 4 ja 5) ja kuvauksessa pyrittiin avoimesti kertomaan, miten tutkimustuloksiin päädyttiin. Tutkimuksen dokumentaatioon ja arvioitavuuteen siis panostettiin. Tutkija myöntää, ettei ollut täysin varma, kuinka paljon analysoinnista olisi pitänyt tarjota esimerkkejä.

Osallistujatarkistus oli merkittävä osa tutkimustulosten luotettavuutta, eli tutkijan tekemät analyysit lähetettiin haastateltaville varmistettavaksi. Kaksi haastateltavaa ei halunnut tutustua analyyseihin. Neljä haastateltavaa antoi kehitysehdotuksen analyyseistä. Kaksi (H2 ja H6) antoivat täsmennysehdotuksia tekstiin helpottamaan niiden tulkintaa, ja kahden (H1 ja H3) korjaukset liittyivät Kyberturvallisuuden ymmärtämisen vastuu -teemaan.

Analyysissa oli alaluokka *Pitääkö uhrin kantaa vastuu rikoksesta*, joka muuttui palautteen jälkeen alaluokaksi *Suojaudutaan rikollisuudelta*. H3:n näkemys oli analysoitu siten, että uhri kantaisi vastuun rikoksesta. H3 kuitenkin korjasi, ettei uhri kanna vastuuta vaan kansalaisilla on varautumisvastuu. H1:n näkemys oli analysoitu siten, että hänen mukaansa vastuu kuulostaa siltä, että uhri kantaa vastuun itse. H1 tarkoitti, että vastuun käsite voi luoda harhaanjohtavan mielikuvan, että uhri on vastuussa, vaikka uhrin pitäisi tietää oikeuksistaan ja mistä hän voi pyytää apua.

Tutkimuksen luotettavuutta ja vahvistettavuutta heikentää se, että monimenetelmällisyyttä ei tehty. Tutkimuksen aineistoa ei siis kerätty useammalla kuin yhdellä menetelmällä, vaikka näin suunniteltiin. Sitä ei tehty, koska tutkimus olisi laajentunut liikaa. Useammalla tavalla kerätty aineisto olisi todennäköisesti syventänyt haastatteluissa nousseita näkemyksiä. Tällöin analysoitavan aineiston määrä olisi kuitenkin kasvanut liian suureksi. On toki huomioitava, että luotettavuusvaraumassa käsiteltiin monimenetelmällisyyden ongelmallisuutta: se ei välttämättä lisää luotettavuutta vaan tutkimuksen syvyyttä.

Palaute teoriaan

Kohderyhmälähtöisyys korostui teoriassa ja tutkimuksen tuloksissa, sillä huomioimalla kohderyhmän tarpeet lisätään ymmärrettävyyttä ja kiinnostavuutta. Tämä oli odotettavissa, koska se huomioitiin kyberturvallisuuden yleistajuistamisen määritelmässä. Teoriassa ja tuloksissa korostettiin myös, ettei yksi viesti sovi kaikille. Tuloksissa voi siis olla ennalta-arvattavia asioita. Tämä hyväksytään, koska opinnäytetyön idea oli myös toimia perustutkimuksena aiheeseen. Opinnäytetyö tarjoaa ymmärrettävää tietoa ilmiöstä kyberturvallisuuden asiantuntijoille – se siis yleistajuistaa viestintää.

Teoriassa todettiin, että kyberturvallisuus on erikoiskieli. Tuloksissa todettiin, että kyberturvallisuuden ja kansalaisen väliin tarvitaan tulkkeja. Tulkin tehtävä on yleistajuistaa erikoiskielen asiat ymmärrettävälle yleiskielelle. Kyberturvallisuuden tulkkaaminen on myös osa asiantuntijan taitoja. Teoriassa tähän viitattiin, kun puhuttiin asiantuntijaviestinnästä.

Tutkimus vahvisti näkemyksen siitä, että kansalaisten on tulevaisuudessa pysyttävä teknologisen kehityksen mukana. Tätä ennakoitiin luvussa 3.5 ja nyt siihen saatiin näkemys myös tämän tutkimuksen haastateltavilta. Tämä yhteys korostaa ymmärrettävän kyberturvallisuuden tarvetta: kansalaisten on kyettävä ymmärtämään ilmiöitä, jotta he voivat pysyä ajan tasalla niistä.

Jatkotutkimusaiheet

Jatkotutkimusaiheina esitetään teemahaastatteluiden vapaan sanan ideoita ja tutkimuksen aikana syntyneitä ajatuksia. Nämä erotetaan toisistaan. Vapaan sanan ideat eivät toimi tutkimustuloksina, tämän takia ne esitetään vasta nyt.

Seuraavat jatkotutkimusaiheet syntyivät haastatteluista:

1. **Viestinnän mittaaminen**: miten kyberturvallisuusviestintää voidaan arvioida ja miten sen vaikutuksia voidaan mitata?
2. **Kansalaisten tietotaitotaso**: millainen keskivertokansalaisen kyberturvaosaaminen on?
3. **Kohderyhmän tunnistaminen ja huomioiminen**: mitkä ovat eri kohderyhmien tarpeet ja miten ne huomioidaan viestinnässä?
4. **Kyberturvallisuuden popularisoiminen**: millä tavalla kyberturvallisuudesta tehdään kiinnostavampaa suurelle yleisölle?
5. **Kansalaisten tavoittaminen**: mitkä viestintäkanavat ja -keinot tehoavat kansalaisiin?

Tutkimuksessa syntynyt jatkotutkimusaihe on: **miten kansalaiset näkevät tämän tutkimuksen tulokset**? Esimerkiksi 1) kokevatko kansalaiset ymmärrettävyyttä lisäävien toimien toimivan, 2) edistävätkö tuloksissa nousseet asiat kiinnostusta ja 3) millainen tarve kyberturvallisuuden yleistajuistamiselle on kansalaisten mielestä? Keskeistä olisi saada kansalaisten näkemykset mukaan tähän ilmiöön. Toisaalta kansalaiset voisivat myös laajemmin kuvailla, mitkä asiat he kokevat vaikeaksi ja miten he haluaisivat oppia asioita.

LÄHTEET

ENISA. 2021. Raising Awareness of Cybersecurity. A Key Element of National Cybersecurity Strategies. PDF-dokumentti. Saatavissa: https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity [viitattu 28.2.2023].

Haney, J. & Lutters, W. 2018. "It's Scary...It's Confusing...It's Dull". How Cybersecurity Advocates Overcome Negative Perceptions of Security. Usenix. PDF-dokumentti. Saatavissa: https://www.usenix.org/system/files/conference/soups2018/soups2018-haney-perceptions.pdf [viitattu 3.3.2023].

Hirsjärvi, S. & Hurme, H. 2022. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. 2., painos. Helsinki: Gaudeamus. E-Kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 23.1.2023].

Juholin, E. 2022. Communicare! Ota viestinnän ilmiöt ja strategiat haltuun. 8., uudistettu painos. Helsinki: Infor / Management Institute of Finland MIF Oy. E-kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 27.2.2023].

Kananen, J. 2019. Opinnäytetyön ja pro gradun pikaopas: Avain opinnäytetyön ja pro gradun kirjoittamiseen. Jyväskylä: Jyväskylän ammattikorkeakoulu. E-kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 21.1.2023].

Kananen, J. 2017. Laadullinen tutkimus pro graduna ja opinnäytetyönä. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kielitoimiston sanakirja: kansantajuinen. 2016. Kotimaisten kielten keskus. WWW-dokumentti. Päivitetty 10.11.2022. Saatavissa https://www.kielitoimistonsanakirja.fi/#/ [viitattu 16.3.2023].

Kielitoimiston sanakirja: yleistajuinen. 2016. Kotimaisten kielten keskus. WWW-dokumentti. Päivitetty 10.11.2022. Saatavissa: https://www.kielitoimistonsanakirja.fi/#/ [viitattu 16.3.2023].

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T., & Salminen, M. 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston kanslia. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja Nro 30/2017. PDF-dokumentti. Saatavissa: http://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213?version=1.0 [viitattu 28.2.2023].

Leskelä, L. & Uotila, E. 2020. Selkokieli saavutettavan viestinnän välineenä. Teoksessa Hirvonen, M. & Kinnunen, T. (toim.) Saavutettava viestintä. Yhteiskunnallista yhdenvertaisuutta edistämässä. Helsinki: Gaudeamus.

Limnéll, J., Alasuutari, M., Candelin, N., Cullen, K., Halonen, O., Helenius, M., Hermunen, T., Lappalainen, J., Latvanen, S., Lindroth, M., Matilainen, T., Palonen, O., Riiheläinen, J., Salminen, M. & Virkkunen, P. 2023. Kyberkansalaistaidot ja niiden kehittäminen Euroopan unionissa. Aalto-yliopiston tutkijaryh-

mä. PDF-dokumentti. Saatavissa: https://cyber-citizen.eu/wp-content/uploads/2023/02/Kyberkansalaistaidot-ja-niiden-kehittaminen-Euroopan-unionissa_FI.pdf [viitattu 1.11.2023].

Linjama, T. 2018. Yleistajuistaminen hoitotyötä tekeville. Tutkimustiedosta näyttöön perustuvaan toimintaan. Jyväskylän ammattikorkeakoulu. Sosiaali-, terveys ja liikunta-ala. PDF-dokumentti. Saatavissa: https://urn.fi/URN:NBN:fi:amk-2018121321283 [viitattu 22.2.2023].

Raevaara, T. 2016. Tajuaako kukaan? Opas tieteen yleistajuistajalle. Tampere: Vastapaino.

Ranta, J. & Kuula-Lummi, A. 2017. Haastattelun keruun ja käsittelyn ABC. Teoksessa Hyvärinen, M., Nikander, P. & Ruusuvuori, J. (toim.) Tutkimushaastattelun käsikirja. Tampere: Vastapaino, 413–426.

Salminen, A. 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan yliopiston julkaisuja. PDF-dokumentti. Saatavissa: https://www.uwasa.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf [viitattu 17.3.2023].

Sandroos, L. 2021. ”Kyberturvallisuus kuuluu kaikille”. Viestinnälliset kehykset yksityishenkilöille suunnatussa tietoturvaviestinnässä. Jyväskylän yliopisto. Informaatioteknologian tiedekunta. Pro gradu -tutkielma. PDF-dokumentti. Saatavissa: http://urn.fi/URN:NBN:fi:jyu-202106083565 [viitattu 4.2.2023].

Erikoiskieli. s.a. Tieteen termipankki. WWW-dokumentti. Saatavissa: https://tieteentermipankki.fi/wiki/Terminologiaoppi:erikoiskieli [viitattu 4.3.2023].

Selkokieli. s.a. Tieteen termipankki. WWW-dokumentti. Saatavissa: https://tieteentermipankki.fi/wiki/Kielitiede:selkokieli [viitattu 4.3.2023].

Yleiskieli. s.a. Tieteen termipankki. WWW-dokumentti. Saatavissa: https://tieteentermipankki.fi/wiki/Kielitiede:yleiskieli [viitattu 4.3.2023].

Tietoarkisto. 2021. Otos ja otantamenetelmät. WWW-dokumentti. Saatavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvanti/otos/otantamenetelmat/ [viitattu 26.2.2023].

Tiililä, U. 2015. Mitä on asiallinen, selkeä ja ymmärrettävä virkakieli? Kielikello 3. Verkkolehti. Saatavissa: https://www.kielikello.fi/-/mita-on-asiallinen-selkea-ja-ymmarrettava-virkakieli- [viitattu 22.8.2023].

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. Uudistettu laitos. Helsinki: Kustannusosakeyhtiö Tammi. E-kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 21.2.2022].

Turvallisuuskomitea. 2018. Kyberturvallisuuden sanasto. PDF-dokumentti. Saatavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf [viitattu 27.2.2023].

Turvallisuuskomitea. 2019. Suomen kyberturvallisuusstrategia 2019. PDF-dokumentti. Saatavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf [viitattu 5.2.2023].

Tutkimuseettinen neuvottelukunta. 2023. Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa. Tutkimuseettisen neuvottelukunnan julkaisuja 2023:2. PDF-dokumentti. Saatavissa: https://tenk.fi/sites/default/files/2023-03/HTK-ohje_2023.pdf [viitattu 17.3.2023].

Vilkka, H. 2021. Tutki ja kehitä. 5., päivitetty painos. Jyväskylä: PS-kustannus. E-kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 21.1.2023].

Liite 1

TEEMAHAASTATTELUN KYSYMYSRUNKO

TEEMA 1: Kyberturvallisuuden yleistajuistaminen kansalaisille

1. Miten kyberturvallisuuden yleistajuistaminen näkyy teidän työssänne?
2. Miten kyberturvallisuuden asiantuntija voi yleistajuistaa kyberturvallisuutta?
3. Miten kyberturvallisuuden ymmärtämisestä tehdään helpompaa kansalaisille?
4. Miten edistetään kansalaisten kiinnostusta oppia lisää kyberturvallisuudesta?
5. Miten varmistetaan, että yleistajuinen viestintä saavuttaa myös heidät, jotka eivät ole kiinnostuneita aiheesta?

TEEMA 2: Kyberturvallisuuden ymmärtämisen vastuu

1. Kenen vastuulla on se, että kansalaiset ymmärtävät kyberturvallisuutta?
   - Pitäisikö vastuun olla jollakin muulla taholla?
2. Millainen vastuu kansalaisilla on omasta kyberturvallisuudestaan?

TEEMA 3: Kyberturvallisuuden yleistajuistamisen tarve

1. Minkälainen tarve kyberturvallisuuden yleistajuistamiselle kansalaisille on teidän kokemuksenne mukaan?
   - Millaisia ongelmia voi syntyä, jos kyberturvallisuuden yleistajuistamiseen ei kiinnitetä huomiota?
2. Mitkä ovat suurimmat haasteet kyberturvallisuuden yleistajuistamiselle?

Loppuun vielä vapaa sana:

- Mikä on sellainen kyberturvallisuuden yleistajuistamiseen liittyvä asia, joka teidän mielestänne kaipaisi enemmän tutkimusta tulevaisuudessa?

Liite 2/1

TEEMAHAASTATTELUN HAASTATELTAVIEN KUVAUKSET

H1:

Yksityisellä sektorilla työskentelevä tietoturvan ja kyberuhkien asiantuntija. Hän on yleistajuistanut kyberturvallisuutta monipuolisesti kansalaisille, ja se on myös tärkeä osa työtä.

H2:

Julkisella sektorilla eri hallinnonaloilla työskennellyt viestinnän asiantuntija. Hänen työssään kyberturvallisuuden yleistajuistamisen kohderyhmä vaihtelee pienestä lapsesta organisaation johtoon.

H3:

Julkisella sektorilla työskentelevä kyberturvallisuuden ja hybridivaikuttamisen asiantuntija. Hän on tukemassa ja levittämässä erityisesti viranomaisviestintää niin, että muut tahot voivat tarjota sitä kansalaisille.

H4:

Korkeakoulussa työskentelevä kyberturvallisuuden opettaja ja tutkija. Hän tekee säännöllisesti ajankohtaisen tiedon välittämistä, asioiden taustoittamista ja opettamista kansalaisille.

H5:

Kyberturvallisuustietoisuuden, -koulutuksen ja -opetuksen tutkija ja asiantuntija. Hänen työssään yleistajuistaminen on koko työn tavoite, ja keskeistä on selvittää, miten kyberturvallisuudesta tehdään ymmärrettävämpää kansalaisille.

H6:

Yksityisellä sektorilla työskentelevä riskienhallinnan ja kyberturvallisuuden asiantuntija. Hänen työssään yleistajuistamista tehdään, kun vuorovaikutetaan asiakkaiden kanssa.

H7:

Yksityisellä sektorilla työskentelevä tietoturva-asiantuntija, tutkija ja kirjailija. Hänen työssään yleistajuistaminen näkyy laajasti kaikessa tekemisessä: kohderyhmät ovat monipuolisia kansalaisista yrityksiin.

H8:

Julkisella sektorilla työskentelevä ennakoinnin ja digitalisaation asiantuntija. Hänen työssään yleistajuistaminen näkyy kykynä muokata globaaleja ilmiöitä ymmärrettäviksi.

H9:

Julkisella ja yksityisellä sektorilla työskennellyt tietosuojan asiantuntija. Hänen työssään yleistajuistamista vaaditaan, koska kansalaisille tuotetun tiedon tulee olla ymmärrettävää.

H10:

Julkisella sektorilla johtoasemassa työskentelevä digitalisaation asiantuntija. Hänen työssään yleistajuistaminen näkyy kansalaisille suunnatussa tuessa ja opettamisessa.

H11:

Julkisella sektorilla työskentelevä terveydenhuollon digiturvallisuuden asiantuntija. Hänen työssään yleistajuistaminen näkyy siinä, että asiakkaiden kanssa pitää kyetä kommunikoimaan ymmärrettävästi.