Lotta Sandroos

”KYBERTURVALLISUUS KUULUU KAIKILLE” – VIESTINNÄLLISET KEHYKSET YKSITYISHENKILÖILLE SUUNNATUSSA TIETOTURVAVIESTINNÄSSÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Sandroos, Lotta
”Kyberturvallisuus kuuluu kaikille” – viestinnälliset kehykset yksityishenkilöille suunnatussa tietoturvaviestinnässä
Jyväskylä: Jyväskylän yliopisto, 2021, 78 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

Tässä tutkielmassa tarkasteltiin yksityishenkilöille suunnattua tietoturvaviestintää. Yksityishenkilöillä ei ole samanlaista ohjaavaa tukiverkostoa tietoturvakäyttäytymisensä tueksi kuin esimerkiksi organisaatioiden jäsenillä, vaikka myös yksityishenkilöt voivat joutua tietoturvaloukkausten uhriksi. Näin ollen tietoturvauhista ja toivotusta käyttäytymisestä tiedottaminen myös yksityishenkilöille on tärkeää. Suomessa yksityishenkilöille tietoturvasta viestii esimerkiksi kansallinen tietoturvatoimija Kyberturvallisuuskeskus, jonka viestintämateriaalit muodostivat tutkielman aineiston. Tutkielmassa aineistoja tarkasteltiin suojelumotivaatioteorian sekä sosiaalisen markkinoinnin teorian luoman teoreettisen viitekehyksen pohjalta, ja tarkoituksena oli tutkia, miten viestintämateriaalit pyrkivät vaikuttamaan kohderyhmän eli yksityishenkilöiden tietoturvakäyttäytymiseen. Analyysi toteutettiin kehysanalyyttisella menetelmällä, jonka avulla tarkasteltiin aineistossa esiintyneitä viestinnällisiä kehyksiä. Viestinnällisten kehysten tutkiminen on tärkeää, jotta voidaan ymmärtää, miten tietoturvasta puhutaan ja minkälaista kuvaa siitä luodaan. Analyysin keskiössä oli kaksi kehystä: suojelumotivaatioteoriaan perustuva uhkapuheen kehys sekä sosiaaliseen markkinointiin nojaava yhteiskunnallisen ulottuvuuden kehys. Analyysissa selvisi, että molempia kehyksiä esiintyi aineistossa lähes yhtä paljon, mutta osittain epätasaisesti eri aineistotyyppien välillä. Aineistossa vedottiin usein uhkien vakavuuteen, alttiuteen uhille sekä minäpystyvyyteen. Sen sijaan sosiaalisen markkinoinnin teoriaan kuuluvaa ajatusta vaihtokaupasta olisi voitu hyödyntää enemmänkin. Tutkimustulokset auttavat tutkijoita ja viestijöitä tunnistamaan tietoturvaviestinnässä hyödynnettäviä viestinnällisiä kehyksiä sekä sitä, miten niitä pystyttäisi käyttämään tietoisesti hyväksi toivotun tietoturvakäyttäytymisen edistämiseksi.

Asiasanat: tietoturvaviestintä, tietoturvakäyttäytyminen, kehysanalyysi, suojelumotivaatio, sosiaalinen markkinointi

ABSTRACT

Sandroos, Lotta
"Cyber security is everyone's business" – Framing in the Information Security Communication targeted at Private Individuals
Jyväskylä: University of Jyväskylä, 2021, 78 p.
Cyber Security, Master's Thesis
Supervisor: Siponen, Mikko

This study was about information security communication targeted at private individuals, who often do not have the same guidance available to support their information security behaviour than members of organisations have. However, private individuals face similar threat of becoming victims of cyber incidents. Therefore, it is important to inform private individuals about cyber threats and the desired information security behaviour. In Finland, the information security communication is done by for example the National Cyber Security Centre, and its materials were analysed in this study. The theoretical framework of the study consisted of the Protection Motivation Theory, and the Social Marketing Theory. The aim of the study was to examine how communication materials try to influence the behaviour of the target audience. With the help of frame analysis, the study examined the frames that appeared in the materials. Studying the frames in communication is important because they can increase understanding of how information security is being talked about. Two frames were prominent in the analysis: the frame of threat speech that was based on the Protection Motivation Theory, and the frame of social dimension that was lead from the theory of Social Marketing. The main findings are the following. Firstly, the number of the appearances of both frames in the material were almost equal, but they were split unevenly between the two material types used in the analysis. Secondly, the most used appeals were the severity, the vulnerability, and the self-efficacy. Instead, the idea of exchange that is a part of Social Marketing could have been utilized even more in the materials. The study and its results can help researchers and practitioners to recognise the frames that appear in the information security communication, and how they could be utilized to achieve the desired information security behaviour.

Keywords: Information Security Communication, Information Security Behaviour, Frame Analysis, Protection Motivation Theory, Social Marketing

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Usein kuulee sanottavan, että ihminen on tietoturvan heikoin lenkki. Yhä useampi tietoturvauhka kohdistuukin juuri ihmisiin (ks. esim. Abawajy 2014). Esimerkiksi tietojenkalastelut ja erilaiset Internetiä hyödyntävät huijaukset ovat tällaisia inhimillisiä heikkouksia hyväksikäyttäviä tietoturvauhkia. Tietoturvauhkia vastaan voi suojautua monenlaisin teknisin toteutuksin, mutta nämäkään eivät pysty aina auttamaan, jos hyökkäyksen kohteena ovat inhimilliset tekijät. Ihmisten tietoturvaosaaminen ja tietoturvatietoisuus ovatkin merkittävässä roolissa niin yksilön kuin yhteiskunnankin tietoturvallisuudessa (Bada, Sasse & Nurse 2019). Tämä merkitys vain kasvanee, jos inhimillisiä heikkouksia hyödyntävät tietoturvauhat lisääntyvät entisestään. Ihmiset eivät välttämättä ymmärrä heihin kohdistuvia tietoturvauhkia, tai niiden yleisyyttä ja vakavuutta, eivätkä he välttämättä edes tajua, että kuka tahansa Internetiä käyttävä voi joutua tietoturvaloukkauksen uhriksi. Voidaankin kysyä, mistä tavallinen kansalainen saa tietoa tietoturvauhista sekä niiltä suojautumisesta? Ja miten tietoturvatietoisuuteen sekä tietoturvakäyttäytymiseen voidaan pyrkiä vaikuttamaan?

Tietoturva ja siitä huolehtiminen ovat tärkeitä nyky-yhteiskunnassamme, jossa yhä useampi omistaa Internetiin yhteydessä olevia älylaitteita ja käyttää sähköisiä palveluja, kuten verkkopankkia (Li & Siponen 2011). Vaikka laitteiden valmistajat ja palvelujen tarjoajat pyrkivät usein ottamaan tietoturvakysymykset huomioon toiminnassaan, jotkin tietoturvaseikat, kuten tarpeeksi vahvojen salasanojen käyttäminen, jäävät kuitenkin kyseisten laitteiden ja palvelujen käyttäjien huolehdittavaksi. Monet organisaatiot edellyttävät jäseniltään määriteltyjen tietoturvanormien noudattamista, ja usein myös kouluttavat työntekijöilleen tai jäsenilleen kyseisen organisaation kannalta olennaisia tietoturvakäyttäytymisen malleja (ks. esim. Anderson & Agarwal 2010). Tietoturva on kuitenkin tärkeää myös yksityishenkilöille, joiden tietoturvakäyttäytymistä ei mikään taho ohjeista tai valvo (ks. esim. Anderson & Agarwal 2010 tai Li & Siponen 2011). Yksityishenkilötkin voivat joutua tietoturvaloukkauksen uhreiksi, erityisesti jos he eivät ymmärrä erilaisia mahdollisia tietoturvauhkia ja niitä vastaan suojautumista.

On hyvä tiedostaa, etteivät tekniset tietoturvaa edistävät toimenpiteet yksin riitä tietoturvallisemman yhteiskunnan rakentamiseen, vaan lisäksi tarvitaan tietoturva-asioista tietoisia, valveutuneita kansalaisia (Abawajy 2014, 238). Samoin tietoturva-asiantuntijoiden panos ei voi korvata jokaisen yksilön tietoturvataitojen ja -tietoisuuden tarvetta (Shaw, Chen, Harris & Huang 2009, 92). Ymmärryksen puutteen onkin nähty olevan merkittävä syy tietoturvan hyvien periaatteiden vastaiseen toimintaan. Tietoisuuden lisäämisen on arvioitu vaikuttavan myönteisesti tietoturvallisemman käyttäytymisen kehittymiseen. (Kortjan & Von Solms 2014, 29) Näin ollen on tarpeen pohtia, miten yksityishenkilöiden tietoisuutta tietoturva-asioista voidaan pyrkiä lisäämään, ja kenen tehtävä se on.

Esimerkiksi yksityishenkilöille suunnatut kurssit, koulutukset, viestintämateriaalit ja kampanjat voisivat auttaa kansalaisten tietoturvaan liittyvän ymmärryksen lisäämisessä (Abawajy 2014). Tässä tutkielmassa perehdytään erityisesti viestintämateriaalien rooliin tietoisuutta edistävässä työssä. Tietoisuuden lisäämistä tietoturva-asioissa on tutkittu aikaisemmin erityisesti kampanjoiden kontekstissa (ks. esim. Bada ym. 2019). Kampanja voidaan määritellä seuraavasti: ”tilapäiset määrätietoiset ponnistelut tiettyyn tavoitteeseen pääsemiseksi, erityisesti ihmisiin vaikuttamiseksi” (Nurmi, Rekiaho & Rekiaho 2009, 223). Viestintä puolestaan voidaan ymmärtää tässä yhteydessä pitkäkestoisemmaksi, jatkuvaksi toiminnaksi. Koska tutkielman aineisto ei koostu ainoastaan kampanjamateriaaleista, on tässä tutkielmassa mielekkäämpää puhua tietoturvaviestinnästä kampanjoiden sijaan. Tutkimalla viestintää ajatuksena on tarkastella laajempaa ja pitkäaikaisempaa toimintaa, sekä luoda siten parempaa ymmärrystä tietoturvaa koskevasta viestinnästä kokonaisuutena. Viestinnän tutkiminen kampanjoiden ohella on tärkeää, koska ihmisten käyttäytymisen muuttuminen etenee yleensä vaiheissa ja vie aikaa (Prochaska & DiClemente 1982). Näin viestinnän tutkiminen on tarkoituksenmukaista, koska viestintä on jatkuvaa ja pitkän tähtäimen toimintaa, toisin kuin lyhytkestoisemmat kampanjat.

Aikaisemmissa tutkimuksissa on tarkasteltu paljon ihmisten tietoturvakäyttäytymistä ja tietoisuutta lisääviä tietoturvakampanjoita, mutta lähtökohtana näissä tutkimuksissa on usein ollut organisaatioiden sisäinen toiminta (ks. esim. Abawajy 2014). Tarve yksityishenkilöiden tietoturvaa koskevan tutkimuksen edistämiselle on kuitenkin tunnustettu (Li & Siponen 2011). Tämä tutkielma yrittää vastata tarpeeseen tarjoamalla lisätietoa yksityishenkilöille suunnatusta tietoturvaviestinnästä. Tietoturvaviestintää on mielekästä tutkia yksityishenkilöiden näkökulmasta, koska heitä ei voi velvoittaa toivottuun tietoturvakäyttäytymiseen samoin kuin organisaation jäseniä, vaan on hyödynnettävä muita keinoja, kuten viestintää, toivotun käyttäytymisen edistämisessä. Lisäksi yksityishenkilöt kohtaavat yhä enemmän tietoturvauhkia sähköisten palvelujen, älylaitteiden ja inhimillisiä heikkouksia hyödyntävien hyökkäysten yhä yleistyessä (ks. esim. Li & Siponen 2011). On helpompi kehittää tehokkaita ja tietoturvatietoisuutta kehittäviä viestejä, kun ymmärretään, mitkä seikat ihmisten tietoturvakäyttäytymiseen vaikuttavat (Anderson & Agarwal 2010, 637).

Koska yksityishenkilöiltä ei voi tietoturvapolitiikan nojalla vaatia tai odottaa tietynlaista käyttäytymistä, ihmisten asenne ja oma-aloitteisuus ovat tärkeässä asemassa tietoturvatietoisuuden ja käyttäytymisen kehittämisessä (Li & Siponen 2011). Ei siis ole yhdentekevää, miten ihmisille tietoturvasta viestitään. Eräs tapa tutkia viestintää ja sen luomaa todellisuutta on kehysanalyysi (ks. esim. Karvonen 2000). Viestien kehystäminen tietyllä tavalla kertoo siitä, miten viestinnällä luodaan tietynlaista kuvaa todellisuudesta, ja miltä tuo todellisuus näyttää (Karvonen 2000, 78). Tutkimalla viestinnässä hyödynnettäviä kehyksiä voidaan saavuttaa parempi ymmärrys siitä, minkälaista kuvaa tietoturvasta luodaan yksityishenkilöiden näkökulmasta, ja miten tavallisille ihmisille puhutaan tietoturvasta. Se, miten tietoturva esitetään viestinnässä kehysten avulla voi vaikuttaa siihen, muuttaako ihminen tietoturvakäyttäytymistään toivottuun suuntaan (Anderson & Agarwal 2010, 637). Onkin hyvin tärkeää, että viestintä onnistuu kehystämään tietoturvaa käyttäytymisen muuttamista edistävällä tavalla. Toisaalta on myös hyvä huomioida, että mikäli viestinnän sävyjä ja viestinnällisiä kehyksiä ei oteta huomioon tai niiden merkitystä ei ymmärretä, voivat vaikutukset olla pahimmillaan toivottua päinvastaiset. Näin ollen viestinnällisten kehysten tarkastelu ja perusteellisempi tutkiminen tietoturvaviestinnän kontekstissa on mielekästä.

Viestinnälliset kehykset voivat muodostua myös tahattomasti, minkä takia niiden tunnistaminen, havaitseminen ja nimeäminen voisivat hyödyntää paitsi tutkimusta, myös tietoturvaviestinnän tekijöitä. Jos viestinnällisiä kehyksiä ei ole tunnistettu, niiden syntyprosessin ymmärtäminen, niiden hallinta ja toimivuuden tarkastelu halutun päämäärän tavoittamisen suhteen voi olla haastavaa. Kun kehyksiä on tunnistettu, niitä voidaan käyttää paremmin tietoisesti hyväksi, minkä lisäksi voidaan tarkastella, miten hyvin kehykset onnistuvat halutun tavoitteen täyttämisessä. Tietoturvaviestinnässä käytettyjen kehysten tunnistaminen ja ymmärtäminen voi tukea myös tietoturva-alan tutkimusta tarjoamalla mahdollisuuden tarkastella, hyödynnetäänkö viestinnässä tieteellisen tutkimuksen valossa tarvittavia asioita käyttäytymiseen vaikuttamiseksi.

Tutkielman tavoitteena on selvittää, minkälaisia viestinnällisiä kehyksiä yksityishenkilöille suunnatussa tietoturvaviestinnässä hyödynnetään. Lisäksi tutkielmassa pyritään selvittämään, miten ihmisten käyttäytymiseen yritetään vaikuttaa näiden viestinnällisten kehysten avulla. Tutkielman tutkimuskysymys on: *Miten viestinnällisten kehysten avulla pyritään vaikuttamaan ihmisten tietoturvakäyttäytymiseen yksityishenkilöille suunnatussa tietoturvaviestinnässä?* Tarkoituksena ei ole selvittää, miten viestintä on onnistunut vaikuttamispyrkimyksessään, vaan tarkastella pyrkimystä vaikuttaa kohderyhmään tiettyjen viestinnällisten kehysten avulla. Tutkimuskysymykseen pyritään vastaamaan hyödyntämällä kehysanalyysia tutkimuksen menetelmänä. Tutkimuksen aineisto koostuu Liikenne- ja viestintävirasto Traficomin alaisen Kyberturvallisuuskeskuksen yksityishenkilöille suunnatuista viestintämateriaaleista. Kansallisena tietoturvatoimijana Kyberturvallisuuskeskus on merkittävä, ellei merkittävin, tietoturvaviestinnän toimija ja kyberturvallisuutta koskevan tiedon lähde Suomessa tavallisen kansalaisen näkökulmasta, minkä takia tietoturva-aiheista viestintää tar-

kastellaan tutkielmassa juuri Kyberturvallisuuskeskuksen tuottamien materiaalien kautta.

Tutkimuskirjallisuus tuntee monia erilaisia teorioita, jotka pyrkivät selittämään ihmisten käyttäytymistä ja toimintaa sekä sitä, miten niihin voidaan yrittää vaikuttaa. Tämän tutkielman teoreettinen viitekehys perustuu ensinnäkin suojelumotivaation teoriaan, jota on tietoturva-alan tutkimuksessa hyödynnetty ihmisen käyttäytymistä ja siihen vaikuttamista selittämään pyrkivänä teoriana (ks. esim. Anderson & Agarwal 2010). Suojelumotivaatioteoriaa on käytetty aikaisemmassa tutkimuksessa erityisesti organisaatiokontekstissa, mutta sen voidaan nähdä soveltuvan myös yksityiskäytön tutkimukseen (Li & Siponen 2011). Tutkielman voidaankin ajatella tarjoavan osaltaan myös ymmärrystä suojelumotivaatioteorian soveltamisesta yksityiskäytön tutkimukseen, minkä tarpeellisuudesta Li ja Siponen (2011, 7) artikkelissaan mainitsevat. Lisäksi tutkielmaan mukaan on valikoitunut sosiaalisen markkinoinnin teoria, jossa tarkastellaan, miten markkinoinnin keinoin voidaan pyrkiä saamaan aikaan laajempaa yhteiskunnallista muutosta (Lefebvre 2013). Molemmat mainitut teoriat tukevat hyvin tutkimuskysymykseen vastaamista: suojelumotivaatioteoria, koska se käsittelee käyttäytymistä sekä käyttäytymisen muuttamista, ja sosiaalinen markkinointi, koska se tarkastelee laajemman sosiaalisen muutoksen aikaansaamista, johon kansalaisille viestimisen voidaan tulkita tässä yhteydessä lukeutuvan.

Tutkielma etenee niin, että seuraavaksi esitellään tutkimuksen kannalta olennaista aiempaa tutkimuskirjallisuutta sekä tutkimuksen teoreettinen viitekehys. Ensimmäiseksi kerrotaan yksityishenkilöiden tietoturvaa koskevasta tutkimuksesta, josta siirrytään esittelemään tietoturvaviestintää, erityisesti tietoturvatietoisuuden lisäämiseen tähtääviä kampanjoita, koskevaa kirjallisuutta. Tämän jälkeen käsitellään tietoturvatietoisuuteen, -käyttäytymiseen ja niihin vaikuttaviin tekijöihin liittyvää aikaisempaa tutkimusta. Lopulta paneudutaan suojelumotivaatioteoriaan sekä sosiaalisen markkinoinnin teoriaan, joihin nojaten tutkimuksen analyysi toteutetaan. Tutkimusasetelman, aineiston sekä menetelmän esittelyn jälkeen vuorossa on varsinainen analyysi, jota seuraavat johtopäätökset päättävät tutkielman.

2 TEOREETTINEN VIITEKEHYS

2.1 Yksityishenkilöiden tietoturva

Tässä alaluvussa esitellään tutkielman kannalta olennaista yksityishenkilöiden tietoturvaa käsittelevää aikaisempaa tutkimusta. Tietoturvakäyttäytymistä sekä tietoturvasta viestimistä on tutkittu aikaisemmin erityisesti organisaatioiden kontekstissa, ja yksityishenkilöiden lähtökohtiin pureutuvaa tutkimusta tarvittaisiin lisää (Li & Siponen 2011). Kuitenkin myös yksityishenkilöiden näkökulmasta on tehty jo jonkin verran tutkimusta. Esimerkiksi Furnell, Bryant ja Phippen (2007) ovat tutkineet yksityishenkilöiden tietoturvaa kotiympäristössä. He epäilivät tutkimuksessaan, ettei yksityishenkilöillä ole riittävää tietoisuutta ja ymmärrystä tietoturvauhista sekä niiltä suojautumisesta, vaikka media uutisoikin tietoturva-aiheista myös yksityishenkilöille (Furnell ym. 2007, 411). Tutkimuksessa selvisi, että valtaosa tutkijoiden kyselyyn vastanneista oli tyytyväisiä tietoturvansa tasoon. Erityisen tyytyväisiä olivat oman tietoteknisen taitotasonsa kehittyneeksi arvioineet vastaajat, kun taas taitotasonsa matalammaksi arvioineet vastaajat olivat tietoturvastaan epävarmempia. (Furnell ym. 412–413)

Furnell ym. (2007, 413) havaitsivat tutkimuksessaan, että vaikka kyselyyn vastanneet arvioivat ymmärtävänsä tietyt tietoturvauhat, he eivät kuitenkaan käytännössä aina olleet tehneet toimenpiteitä näitä uhkia vastaan. Toisin sanoen, ihmiset arvioivat ymmärtävänsä tietoturvauhkia, mutta päättävät kuitenkin olla tekemättä tarvittavia toimia suojautuakseen niiltä. Tutkijat arvioivat tämän johtuvan joko siitä, että ihmiset yliarvioivat tietoturvauhkia koskevan ymmärryksensä, tai eivät jostain syystä koe uhkien koskisivan heitä niin paljon, että sille tarvitsisi tehdä jotain (Furnell ym. 2007, 413). Kun vastaajilta kysyttiin, pitäisikö yksityishenkilöiden ottaa vastuuta omien laitteidensa suojaamisesta tietoturvauhkia vastaan, lähes kaikki vastaajat vastasivat myöntävästi. Vahvimmin vastuun ottamisen puolesta puhuivat omat tietotekniset taitonsa edistyneiksi arvioineet vastaajat, joista jopa kuusikymmentä prosenttia oli vahvasti samaa mieltä väitteen kanssa. Toisaalta on kiinnostavaa, että samaisesta edistyneiden vastaajaryhmästä olivat peräisin myös ainoat vahvasti eri mieltä olevat

vastaukset (2 prosenttia kyseisen viiteryhmän vastaajista). Lisäksi omat tietotekniset taitonsa alkeellisiksi arvioineista vastaajista jopa 22 prosenttia vastasi kysymykseen 'en osaa sanoa', kun taas muissa viiteryhmissä 'en osaa sanoa' -vastausvaihtoehto keräsi vain muutaman prosentin edestä vastaajia. Tutkijat päättelivätkin, että ihmisten tietoisuutta pitäisi aktiivisesti lisätä, jos vastuun tietoturvasta ajatellaan lankeavan yksityishenkilöille. (Furnell ym. 2007, 414)

Tutkimus paljastaa myös, miten yksityishenkilöt ovat monesti oman onnensa nojassa tietoturva-asioissa: 70 prosenttia vastaajista ilmoitti, etteivät he olleet saaneet tietoturvaan liittyviä neuvoja tai tietoja laitteitaan ostaessaan. Kysyttäessä lähteitä, joista henkilöt etsivät tietoa tietoturva-asioista, suosituimpia tiedonlähteitä vastaajien keskuudessa olivat IT-ammattilaiset (43% vastaajista ilmoitti lähteeksi), julkinen tieto tai verkkosivut (43%) sekä ystävät tai sukulaiset (41%). Verkkosivuja tietolähteenä käyttäneet vastaajat laitettiin arvioimaan myös brittiläisten tietoturva-asioita ohjeistavien verkkosivujen tunnettuutta sekä hyödyllisyyttä. Valtaosa erityisesti valtionhallinnon ylläpitämistä verkkosivuista oli vastaajille suhteellisen tuntemattomia, mutta yleisesti verkkosivuilla vierailleista noin puolet koki ne myös hyödyllisiksi. Toisaalta tutkijat huomauttavat, että verkkosivujen tunnettuus vaikutti korostuneen tietotekniset taitonsa edistyneiksi arvioineiden vastaajien joukossa, mikä saattaa viitata siihen, etteivät tietoturvaohjeita jakavat verkkosivut onnistuisi tavoittamaan yhtä hyvin niitä, jotka arvioivat taitotasonsa heikommaksi. (Furnell ym. 2007, 415) Kun ihmisiltä kysyttiin, kenen puoleen he voisivat kääntyä tietoturvaloukkauksen tapahtuessa, puolet vastaajista vastasi, ettei tiedä (Furnell ym. 2007, 416).

Syitä tietoturvallisen toiminnan laiminlyömiseen olivat tutkimuksen mukaan esimerkiksi tietoturvapalvelujen ja -sovellusten liian kalliit hinnat, tietämättömyys miten omaa laitetta voi suojata, sekä kokemus siitä, että tietoturva estää laitteen käyttöä. Eri viiteryhmien välillä oli kuitenkin eroja. Esimerkiksi vähemmän edistyneiksi itsensä kokeneet vastaajat arvioivat taitoihinsa ja osaamiseensa liittyvien tekijöiden estävän tietoturvallista toimintaa. Sen sijaan edistyneemmät vastaajat kokivat palvelujen hintavuuden sekä tietoturvan asettamien käytön esteiden olevan pääsyitä sille, miksi he laiminlyövät tietoturvaa edistäviä toimenpiteitä. (Furnell ym. 2007, 416) Furnell ym. (2007, 417) pitävätkin erityisen tärkeänä sitä, että enemmän huomiota kiinnitettäisi yksityishenkilöiden tietoturvatietoisuuden kehittämiseen.

Myös Anderson & Agarwal (2010) ovat tutkineet ihmisten tietoturvakäyttäytymistä kotiympäristössä. He havaitsivat tutkimuksessaan, että ihmisten omia laitteitaan koskevaan tietoturvakäyttäytymiseen vaikuttavat esimerkiksi subjektiiviset normit, eli ihmisen arvio siitä, miten hänen muiden mielestä tulisi käyttäytyä. Toisaalta Internetin kontekstissa ihmisten tietoturvakäyttäytymiseen havaittiin vaikuttavan sen sijaan deskriptiiviset normit, eli ihmisten havainnot muiden ihmisten käyttäytymisestä. Lisäksi yksilön positiivinen asenne ja usko omiin kykyihin toimia tarvittavalla tavalla lisäävät todennäköisyyttä tietoturvallisempaan käyttäytymiseen. Tutkijat havaitsivat omistajuuden tunteen vaikuttavan yksilön aikeisiin suojata omistuksen kohdetta, esimerkiksi tietokonetta. (Anderson & Agarwal 2010, 628) Kotiympäristön käyttäjien tietotur-

vakäyttäytymistä koskeviin asenteisiin vaikuttaa edellä mainittujen tekijöiden lisäksi se, miten huolissaan henkilö on tietoturvauhista (Anderson & Agarwal 2010, 630).

Li ja Siponen (2011) esittävät, että ihmisen käyttäytyminen voi vaihdella sen mukaan, toimiiko hän kotona, työpaikalla tai jossain muussa kontekstissa. Ihminen päättää itse, miten käyttäytyy toimiessaan kotona omilla laitteillaan, kun taas työoloissa työnantajan laitteita käyttäessään hänen on noudatettava työnantajan antamia ohjeita. Tietoturvakäyttäytyminen voikin vaihdella kontekstin ja käyttötarkoituksen mukaan. (Li & Siponen 2011, 5) Li ja Siponen (2011, 5–6) ovat määritelleet neljä erilaista käytön tapaa, jotka jakautuvat kahteen eri ulottuvuuteen. Ensinnäkin on paikkaulottuvuus, eli toimitaanko kotiympäristössä vai työpaikalla. Näin voidaan huomioida myös kotoa käsin tehtävä etätyö. Toinen ulottuvuus on käyttötarkoitus, eli käytetäänkö laitteita omiin asioihin vai työasioiden hoitamiseen. Tässäkin yhteydessä huomioidaan, että ihminen voi käyttää esimerkiksi työtietokonettaan omien asioidensa hoitamiseen. Neljästä käytön tavasta ensimmäinen koskee työpaikalla tehtävää työtä, ja toinen työskentelyä kotoa. Kolmas käyttötapa on työpaikalla tehtävät työhön liittymättömät asiat, ja neljäs puolestaan on henkilökohtainen käyttö kotioloissa. (Li & Siponen 2011, 5–6) Tämän tutkielman puitteissa olennaisin on neljäs käytön tapa, eli henkilökohtainen käyttö kotona.

Lin ja Siposen (2011) mukaan kotioloissa tapahtuva henkilökohtainen käyttö eroaa työpaikalla tapahtuvasta työkäytöstä siinä, miten paljon erilaisia mahdollisuuksia on tarjolla. Kotioloissa henkilökohtaisessa käytössä ihminen voi käyttää laitteitaan ja Internetiä eri tarkoituksiin, joista moni näyttäytyy varsin houkuttelevana, kuten pelaaminen, verkkokeskusteluihin osallistuminen, verkkokaupoista osteleminen tai erilaisten sisältöjen lataaminen. Ottaen huomioon nämä mahdollisuuksien ja käyttötarkoitusten erot, ihmisen tietoturvaa koskevat asenteet ja käyttäytyminen saattavat olla hyvinkin erilaisia kuin työoloissa. (Li & Siponen 2011, 6) Näiden mahdollisten eroavaisuuksien takia Li ja Siponen peräänkuuluttavat lisää tutkimusta henkilökohtaisen kotikäytön näkökulmasta. Tietoturvakäyttäytymistä on aikaisemmin tutkittu kotikäyttöä enemmän työkäytön näkökulmasta, mutta henkilökohtaista kotikäyttöä koskevan tutkimuksellisen ja käytännön ymmärryksen kehittämiseksi kotikäyttöä olisi hyvä tutkia nykyistä enemmän. (Li & Siponen 2011, 2)

Li ja Siponen (2011, 6) esittävät, että kontekstuaaliset tekijät voivat vaikuttaa ihmisten asenteisiin ja käyttäytymiseen. Huomionarvoista on esimerkiksi, etteivät yksityishenkilöt saa tietoturvatietoisuutta kehittävää tietoturvakoulutusta samalla tavalla kuin työntekijät työpaikoillaan. Näin yksityishenkilöt joutuvat monesti turvaamaan omaehtoiseen opetteluun sekä kokemuksen kautta saatuihin oppeihin. Pahimmassa tapauksessa tietoisuus voi kehittyä vasta tositilanteen tullen, kun ihminen törmää johonkin tietoturvauhkaan, kuten haittaohjelmiin. (Li & Siponen 2011, 6) Yksityishenkilöiden osaaminen voikin perustua suuressa määrin heidän omaan aktiivisuuteensa ja oma-aloitteisuuteensa tietoturva-asioissa. Myös osaaminen on tärkeässä roolissa, koska yksityiskäytöstä puuttuu työpaikkojen monesti tarjoama tekninen tuki (Li & Siponen 2011, 7).

On hyvä huomioida, että kontekstuaalisten erojen takia kaikki organisaatioiden tutkimuksessa hyödynnetyt teoriat eivät välttämättä toimi yhtä hyvin yksityiskäytön näkökulmasta. Esimerkiksi peloteteoria perustuu ajatukseen muodollisista sanktioista, joita ei yksityiskäytön yhteydessä juurikaan ole (Li & Siponen 2011, 7). Tämän tutkielman kontekstissa huomionarvoista on erityisesti suojelumotivaatioteorian sopivuus yksityiskäytön tutkimiseen. Suojelumotivaatioteoria soveltuu Lin ja Siposen (2011, 7) mukaan peloteteoriaa paremmin kotikäytön kontekstiin, vaikka siinäkin voi esiintyä yksityiskäytön näkökulmasta puutteita. Li ja Siponen (2011, 7) esittävätkin oletuksen, että erilaiset pelkoon viittaavat tekijät saattavat olla tehokkaampia työkäytön kuin kotikäytön kontekstissa. Oletuksen todentaminen vaatii kuitenkin kotioloissa tapahtuvan yksityiskäytön lisätutkimusta, jonka tarvetta Li ja Siponen (2011) korostavatkin artikkelissaan. Vaikka tämän tutkielman yhteydessä ei pystytä vastaamaan esitettyyn oletukseen, tarjoaa tutkielma kuitenkin toivottua lisänäkökulmaa suojelumotivaatioteorian hyödyntämiseen yksityiskäytön kontekstissa. Tutkielmassa joudutaan kuitenkin jonkin verran turvautumaan lähinnä organisaatiokontekstin tutkimuksiin yksityiskäytön näkökulmasta tehtyjen tutkimusten vähäisyyden vuoksi.

2.2 Tietoturvaviestintä ja -kampanjat tietoisuuden edistäjinä

Tämän alaluvun tarkoituksena on esitellä erityisesti tietoturvaa koskevan viestinnän kannalta merkittävää aikaisempaa tutkimusta. Lisäksi luvussa käsitellään tietoturvatietoisuuteen linkittyvää tutkimuskirjallisuutta, koska viestintää voidaan hyödyntää tietoisuuteen vaikuttamisessa. Alaluvussa esitellään niin viestin välittämisen keinoja, tietoturvakampanjoiden onnistumiseen vaikuttavia tekijöitä, kuin kehystämisen merkitystä kampanjoissa. Kuten edellä jo mainittiin, tietoturvaviestintää on aikaisemmassa tutkimuksessa tutkittu lähinnä kampanjoiden kautta, minkä takia osiossa joudutaan nojaamaan kampanjoita koskevaan tutkimuskirjallisuuteen laajempaa tietoturvaviestintää käsittelevän tutkimuksen vähyyden vuoksi. Kampanjat määriteltiin jo aiemmin tässä tutkielmassa tilapäisiksi ponnisteluiksi, joiden tarkoituksena on usein vaikuttaa ihmisten toimintaan, kun taas viestintä ymmärretään tämän tutkielman kontekstissa kampanjaa pitkäkestoisemmaksi, pysyvämmäksi toiminnaksi. Kampanjoita on hyödynnetty erityisesti organisaatioiden sisällä lisäämään organisaation jäsenien tietoisuutta tietoturvasta, ja tietoturvakampanjat ovatkin yleisesti hyödynnetty tapa kertoa organisaation jäsenille tietoturvavaatimuksista ja oikeaoppisesta tietoturvakäyttäytymisestä (ks. esim. Bada ym. 2019).

Tietoturvatietoisuuden voidaan määritellä tarkoittavan yksilön ymmärrystä tietoturvan merkityksestä sekä omasta roolistaan tietoturvan toteutumisessa (Shaw ym. 2009, 92). Tietoturvatietoisuutta edistävän työn tavoitteena on vakiinnuttaa ja edistää hyviä tietoturvakäytäntöjä muuttamalla ihmisten asenteita (Abawajy 2014, 239). Tietoturvatietoisuuteen viitataan englanninkielisessä tutkimuskirjallisuudessa usein termillä *Information Security Awareness* (ks. esim.

Siponen 2000). Tietoturvatietoisuuden ja -käyttäytymisen tutkimukseen liittyy kuitenkin muitakin termejä, joita on tässä kohtaa hyvä selventää. Esimerkiksi organisaatioiden näkökulmasta on usein syytä puhua ohjeiden noudattamatta jättämisestä, mistä on käytetty englanninkielisessä tutkimuksessa käsitettä *Security Policy Compliance* (Puhakainen & Siponen 2010). Organisaatioiden yhteydessä on käytetty myös termiä *Security Policy Violations*, jolla viitataan niin ikään tietoturvapolitiikkojen antamien ohjeiden rikkomiseen tai noudattamatta jättämiseen (Siponen & Vance 2012). Sen sijaan esimerkiksi D'arcy, Hovav ja Galletta (2009) hyödynsivät tietoturvatietoisuutta koskevassa ja peloteteoriaa soveltavassa tutkimuksessaan termiä *Information Systems Misuse*, jolla viitataan organisaation sisäisiin väärinkäytöksiin. Samoin peloteteorian kontekstissa esimerkiksi Straub (1990, 257) on puolestaan käyttänyt käsitettä *Computer Abuse* viittaamaan harkitusti tehtyihin rikkomuksiin normeja ja ohjeita vastaan. *Awareness*-termi vaikuttaa kuitenkin olevan yleisimmin hyödynnetty nimenomaan yksilöiden tietoisuutta edistävän toiminnan sekä kampanjoiden tutkimuksessa (ks. esim. Bada ym. 2019), minkä takia sitä käytetään myös tässä tutkielmassa.

Tietoisuuden lisäämistä on pidetty tärkeänä osana tietoturvan toteutumisen edistämistä, koska hyökkääjien tiedetään usein valitsevan helppoja reittejä ja keinoja hyökkäykselle, ja nämä usein liittyvät inhimillisiin tekijöihin, kuten huolimattomaan salasanakäyttäytymiseen tai kyvyttömyyteen tunnistaa tietojenkalasteluviestejä (Abawajy 2014, 237). Heikko tietoisuus tietoturvauhista sekä hyvistä tietoturvan toimintamalleista on nähty yhtenä tietoturvan toteutumisen merkittävimmistä puutteista (Shaw ym. 2009, 93). Näin ollen, organisaatioille tietoturvatietoisuuden edistäminen näyttäytyy keinona hallita inhimillisiä heikkouksia, joita tietoturvakäyttäytymiseen voi liittyä (Abawajy 2014, 238). Haasteena tietoturvatietoisuutta lisäämään tähtäävissä toimissa, kuten kampanjoissa, on tietoisuuden realisoituminen tietoturvallisemmaksi käyttäytymiseksi (Shaw ym. 2009, 92). Käyttäytymisen ja asenteiden muuttumista voitaisiin tietyssä mielessä pitää tietoisuutta edistävien toimien, myös kampanjoiden, onnistumisen mittarina.

Tietoturvakampanjoita voidaan tarkastella eri näkökulmista sen perusteella, mitä viestin välittämisen keinoja niissä hyödynnetään, tai millä tavoin ne pyrkivät vaikuttamaan kohdeyleisöönsä. Kampanjoiden onnistumiseen, eli miten hyvin ne onnistuvat vaikuttamaan halutulla tavalla kohdeyleisöönsä, vaikuttavatkin monenlaiset seikat. Seuraavissa alaluvuissa esitellään kampanjoita ja viestintää koskevaa aikaisempaa tutkimuskirjallisuutta.

2.2.1 Viestin välittämisen keinot

Kampanjoiden onnistumiseen vaikuttaa tutkimusten mukaan esimerkiksi ne viestin välittämisen tavat[1], joilla kampanjaa toteutetaan (Shaw ym. 2009, 99). Abawajy (2014) on jakanut viestin välittämisen keinot kuuteen eri kategoriaan,

[1] eng. delivery methods, oma suomennos.

jotka ovat tavanomaiset keinot, ohjaajavetoiset keinot, online-keinot, pelilliset keinot, videolliset keinot sekä simulaatiolliset keinot. Tavanomaiset keinot viittaavat sekä elektronisiin, esimerkiksi uutiskirjeisiin, että perinteisiin paperisiin materiaaleihin, kuten julisteisiin ja tiedotelehtisiin. Näiden haasteena on epävarmuus siitä, ovatko tavanomaisin keinoin välitetyt viestit tulleet huomatuiksi, saati sisäistetyiksi. (Abawajy 2014, 240–241) Näin tavanomaisten keinojen heikkous piilee niiden passiivisessa, oma-aloitteisuutta vaativassa luonteessa. Ohjaajavetoiset keinot sen sijaan pystyvät välttämään tämän ongelman. Nimensä mukaisesti ohjaajavetoiset keinot perustuvat asiantuntijan pitämiin, ohjattuihin koulutustapahtumiin. Menetelmän vahvuus on sen vuorovaikutteisuudessa, jolloin ohjaaja pystyy mukauttamaan viestiään kohdeyleisölle sopivaksi. Ohjaajavetoisten keinojen heikkoudet muihin keinoihin verrattuna liittyvät sen kalleuteen sekä onnistumisen riippuvuuteen ohjaajan kyvystä luoda kaikkia kiinnostava ja innostava oppimisympäristö. (Abawajy 2014, 241)

Online-keinoilla viitataan moniin erilaisiin viestin välittämisen tapoihin, kuten massasähköposteihin, online-keskusteluihin, blogeihin ja muuhun online-pohjaiseen multimediaviestintään (Abawajy 2014, 241). Pelilliset keinot tarkoittavat puolestaan pelillisiä ominaisuuksia sisältäviä viestimisen tapoja. Pelilliset menetelmät ovat viestin vastaanottajaa aktivoivia ja vuorovaikutteisia, ja niitä on hyödynnetty esimerkiksi tietojenkalasteluviestien tunnistamisen opettamiseen. Videolliset keinot ovat ohjaajavetoisia keinoja kustannustehokkaampia, mutta tarjoavat mahdollisuuden hyödyntää visuaalisuutta ja audioperusteisia keinoja viestin välittämiseen. Kohdeyleisö voi perehtyä viesteihin omaan tahtiinsa, keskittyä vain heille relevantteihin aiheisiin sekä katsoa tarpeen tullen jotain kohtia uudelleen. (Abawajy 2014, 242) Lopulta, simulaatiolliset keinot tarkoittavat tietoisuutta lisääviä, opetuksellisia menetelmiä, joissa osallistujille simuloidaan oikeaa tilannetta, esimerkiksi lähettämällä simuloitu tietojenkalasteluviesti ja tarkastella osallistujien reagointia siihen (Abawajy 2014, 242).

Samassa tutkimuksessaan Abawajy tutki myös eri viestin välittämisen menetelmien, erityisesti tavanomaisten, pelillisten ja videollisten keinojen, tehokkuutta sekä kohdeyleisön näkemyksiä siitä, mikä menetelmä oli heille mieluisin (Abawajy 2014). Menetelmien tehokkuutta mitattiin Abawajyn tutkimuksessa arvioimalla, kuinka hyvin osallistujat pystyivät tunnistamaan tietojenkalasteluviestejä eri menetelmin suoritettujen koulutuskampanjoiden jälkeen. Kaikki kolme keinovalikoimaa, eli tavanomaiset, pelilliset ja videolliset, paransivat osallistujien kykyä tunnistaa tietojenkalastelua. Tavanomaiset, tekstilliset menetelmät onnistuivat tasaisesti eri koeasetelmissa, kun taas pelillisten ja videollisten keinojen tehokkuus vaihteli eri asetelmissa. (Abawajy 2014, 245) Osallistujilta kysyttäessä suosituimmaksi menetelmäksi testatuista kolmesta keinosta osoittautuivat videolliset keinot, kun taas tavanomaiset, tekstiperustaiset keinot saavuttivat toiseksi suurimman suosion. Pelillisten keinojen suosio oli yllättävän alhainen, jopa suosikistaan epävarmoja vastaajia oli enemmän kuin pelillisiä keinoja suosivia vastaajia. Abawajyn mukaan videollisten menetelmien suosio erityisesti tavanomaisten, tekstiperustaisten keinojen ohi saattaa johtua videoiden mahdollistamasta paremmasta oppimiskokemuksesta, kun

tietoa on saatavilla sekä visuaalisessa että kielellisessä muodossa. Toisaalta sekä videolliset että tavanomaiset keinot välittävät tietoa helpommin jäsenneltävissä ja ymmärrettävissä olevassa muodossa, minkä vuoksi Abawajy olettaa niiden voittaneen pelilliset keinot suosiossa. (Abawajy 2014, 246) Abawajy ehdottaakin, että kaikkia hänen tutkimuksessaan testaamiaan kolmea viestin välittämisen menetelmää tulisi käyttää yhdessä parhaimman mahdollisen tuloksen saavuttamiseksi. Lisäksi Abawajy huomauttaa, että yhden ja saman viestin välittämisen mallin (niin kutsuttu *one-size-fits-all* -mallin) ei voida olettaa toimivan kaikille yhtä lailla, ja että viestin välittämisen keinot voisivat hyvin vaihdella esimerkiksi opetettavan aihepiirin mukaan. Kaiken kaikkiaan olennaista tietoisuuden lisäämisessä on Abawajyn mukaan se, että viestit pysyvät johdonmukaisina, mutta viestin välittämisen menetelmät joustaisivat tarpeen mukaan. (Abawajy 2014, 247)

2.2.2 Kampanjoiden onnistuminen ja epäonnistuminen

Kuten aikaisemmin jo todettiin, kampanjoiden onnistumisen kannalta merkitystä on esimerkiksi sillä, mitä viestin välittämisen tapoja kampanjassa hyödynnetään (Shaw ym. 2009, 99). Bada ym. (2019, 9) listaavat puolestaan tutkimuksessaan useita muita toimenpiteitä kampanjoiden onnistumisen parantamiseksi. Kampanjoiden tulisi olla ammattitaitoisesti valmisteltuja, ja kampanjamateriaaleissa olisi hyvä välttää liiallista pelon lietsomista. Kampanjan pitäisi olla kohderyhmälle suunnattu, ja kampanjassa ehdotettujen toimenpiteiden tulisi olla kohdeyleisön toteutettavissa (Bada ym. 2019, 9). Toisin sanoen kampanjan pitäisi ottaa antamissaan ohjeistuksissa huomioon esimerkiksi kohdeyleisön taitotaso, koska liian vaikeita ja yksityiskohtaisia ohjeita voi olla vaikea seurata ilman tarvittavaa teknistä osaamista. Lisäksi, kun kampanja onnistuu saamaan aikaan muutosta ihmisten käyttäytymisessä, ihmisille olisi hyvä tarjota palautetta heidän toimistaan (Bada ym. 2019, 9). Myös kulttuuriset erot olisi hyvä ottaa huomioon kampanjoita suunnitellessa (Bada ym. 2019, 9).

Kampanjoiden onnistumista heikentävät puolestaan epämääräiset ja monitulkintaiset varoittelut, liian monimutkaiset ohjeistukset sekä pelkoa lietsovat viestit. Liialliset varoittelut voivat johtaa ajatukseen, ettei suojautumisessa ole mitään mieltä, kun taas liian epäselvät ohjeistukset voivat jättää epäselvyyksiä siitä, miten tulisi toimia. Viestien liiallinen pelon lietsominen voi puolestaan lisätä stressiä, jolloin ihmisessä saattaa herätä henkinen vastareaktio. (Bada ym. 2019, 3) Jatkuva varovaisuus, jota tietoturvallisen käytöksen voidaan ymmärtää edellyttävän, on niin ikään seikka, joka voi lisätä yksilön kokemaa stressiä. Joskus tietoturva voidaan nähdä myös haluttua toimintaa kieltävänä esteenä. Esimerkiksi henkilö voi haluta vierailla verkkosivulla, jota virustorjunta pitää haitallisena, jolloin houkutus ohittaa virustorjunnan varoitukset voi kasvaa liian suureksi. (Bada ym. 2019, 4) Mitä enemmän viestejä henkilö vastaanottaa tiettyä asiaa, esimerkiksi jotain tietoturvauhkaa, koskien, sitä vaikeampaa on arvioitu henkilön käyttäytymisen muuttamisen olevan (Bada ym. 2019, 6). Tämä arvio

voisi perustua ajatukseen, että ihminen turtuu jatkuviin viesteihin. Lisäksi viestien ollessa keskenään epäjohdonmukaisia, ei kohdeyleisö välttämättä osaa tunnistaa, mitä siltä odotetaan. Tämä voi edelleen johtaa passiivisuuteen.

Kajzerin, D'Arcyn, Crowellin, Striegelin, ja Van Bruggenin (2014) mukaan suostuttelevan tietoturvakampanjan tulisi ottaa huomioon kohdeyleisön henkilökohtaiset ominaisuudet onnistuakseen vaikuttamaan ihmisten käyttäytymiseen halutulla tavalla. Heidän tutkimuksensa mukaan erityisesti ihmisten persoonallisuustekijät vaikuttavat siihen, kuinka hyvin tietoisuutta edistävien kampanjoiden viestit onnistuvat vaikuttamispyrkimyksissään (Kajzer, D'Arcy, Crowell, Striegel, & Van Bruggen 2014, 69). Näin ollen, erilaisille ihmisille toimivat erilaiset viestit, jolloin kampanjan onnistuminen voi riippua myös siitä, miten hyvin kampanja pystyy ottamaan erilaiset ihmiset ja heidän persoonallisuutensa huomioon.

Kuten aikaisemmin jo mainittiin, Kajzer ym. (2014, 69) huomauttavat myös, että viestien mukauttaminen kohdeyleisön ominaisuuksien, erityisesti persoonallisuuden, mukaan voisi edesauttaa viestinnän onnistumista. Viestinnän ei näin ollen voida olettaa vaikuttavan kaikkiin ihmisiin samalla tavalla, mikä esimerkiksi organisaatioiden tulisi ottaa huomioon tietoturvatietoisuutta edistävässä työssään (Kajzer ym. 2014, 70). Viestien mukauttaminen erilaisille persoonallisuustyypeille sopiviksi vaikuttaa kuitenkin paljon resursseja vaativalta työltä. Lisäksi se asettaa viestinnän tekijöille haasteita, koska tämä lähestymistapa edellyttäisi heiltä hyvin pitkälle menevää kohdeyleisönsä henkilökohtaisten ominaisuuksien tuntemista.

Korpelan (2015, 73) mukaan tietoturvakampanjan epäonnistumiseen vaikuttavat myös kyvyttömyys tunnistaa riskialttiimmat henkilöt sekä kyvyttömyys ymmärtää, miten ihmiset oikeastaan oppivat tietoturvaan liittyviä asioita. Korpela huomauttaa, että esimerkiksi ihmisen asemaan organisaation sisällä perustuva tietoturvakouluttaminen ei ole riittävä lähestymistapa, vaan aseman sijaan pitäisi kiinnittää enemmän huomiota siihen, mikä on kunkin henkilökohtainen riskitaso esimerkiksi työtehtävien luonteen myötä. Henkilökohtaisen riskin tasoon vaikuttaa esimerkiksi henkilön Internet-käyttäytyminen sekä hänen roolinsa organisaatiossa. (Korpela 2015, 73) Lisäksi Korpela pitää yleistä *one-size-fits-all* -lähestymistapaa kohdeyleisön henkilökohtaisia oppimistapoja heikosti huomioon ottavana (Korpela 2015, 74). Ihmisten erilaiset ominaisuudet ja tavat oppia olisi hyvä ottaa paremmin huomioon, jos tietoturvakampanjan halutaan onnistuvan. Tietoturvakampanjat sekä -koulutukset tulisi räätälöidä oppimistapojen lisäksi kohderyhmän aseman, työtehtävien, oppimistarpeiden, kiinnostuksen kohteiden sekä teknologiasuhteensa mukaan. Huomioitavia asioita ovat esimerkiksi koulutusmenetelmät, koulutuksissa tai kampanjoissa katettavat teemat, kohderyhmän taitotaso ja materiaalin muuttuminen kehityksen myötä, tietoturvaväsymyksen välttäminen sekä keinot, joilla voidaan mitata koulutuksen tai kampanjan kykyä lisätä tietoisuutta ja innostusta. (Korpela 2015, 74)

2.2.3 Kehystämisen merkitys viestinnän onnistumisessa

Kajzer ym. (2014) ovat määritelleet erilaiset ihmisten toimintaan vaikuttamaan pyrkivät suostuttelevat viestit sen mukaan, mihin periaatteisiin ne yrittävät vedota. Näitä suostuttelun periaatteita ovat Kajzer ym. (2014, 65) mukaan pelote, moraali, katumus, palaute ja kannuste. Pelotteella tarkoitetaan viestejä, jotka vetoavat kiellettyä käyttäytymistä vastaan asetettuihin sanktioihin. Peloteviestit perustuvat ajatukseen, että ihmiset ovat rationaalisia toimijoita, jotka pyrkivät maksimoimaan voitot ja minimoimaan kustannukset. (Kajzer ym. 2014, 65) Moraaliviestit puolestaan pohjautuvat oletukseen, jonka mukaan ihmisten päätöksenteko perustuu moraalisiin periaatteisiin ja arvoihin (Kajzer ym. 2014, 66). Katumusviestejä on perusteltu sillä, että ihmiset pyrkivät ennakoimaan toimintansa lopputuloksia, ja välttämään ennakoituja epätoivottuja lopputuloksia, kun taas kannusteviestit pohjautuvat ihmisten motivoimiseen toivottuun käyttäytymiseen kannustimien ja palkintojen avulla. Palauteviesteissä ajatuksena on, että ihmisten toimintaa seuraa palaute, ja hyvää palautetta saadessaan ihminen jatkaa toimintaansa, kun taas kielteinen palaute saa ihmisen muuttamaan käyttäytymistään. (Kajzer ym. 2014, 66)

Bada ym. (2019) huomauttavat, ettei tietoisuuden lisäämiseen tähtäävien kampanjoiden pidä tyytyä vain viestimään kohdeyleisölle minkälaista toivottu tietoturvakäyttäytyminen on, vaan niiden pitäisi pyrkiä myös auttamaan kohdeyleisöä ymmärtämään, miten olennaisia tietoturvakysymykset ovat heidän kannaltaan ja miten välitettyyn tietoon tulisi suhtautua. Kampanjan onnistumisen kannalta olennaisia seikkoja ovat esimerkiksi materiaalien kiinnostavuus, ajankohtaisuus ja helppous. (Bada ym. 2019, 2) Kampanjaviestit ovat yleensä tehokkaampia, jos ne on kehystetty sopimaan yhteen kohdeyleisön kognitiivisten ja motivaatiollisten piirteiden sekä tunteisiin liittyvien piirteiden kanssa (Bada ym. 2019, 4). Tässä yhteydessä juuri viestien kehystäminen tietyllä tavalla voi vaikuttaa viestien tehokkuuteen ja siten koko tietoisuutta lisäävän kampanjan onnistumiseen, minkä takia juuri viestinnällisiä kehyksiä on merkityksellistä tarkastella. Bada ym. (2019, 6) pitävätkin erityisesti viestintää tietoturvatietoisuutta edistävän kampanjan onnistumisen kannalta olennaisena.

Tietoturvaa koskevien viestien kehystämistä ovat tutkineet myös Anderson ja Agarwal (2010). He perehtyivät tutkimuksessaan siihen, miten positiivisesti tai negatiivisesti kehystetyt viestit, sekä yksilötasoon tai yhteisötasoon kehystetyt viestit koettiin tietoturvakäyttäytymisen kannalta (Anderson & Agarwal 2010, 633). Positiivisesti kehystetyt viestit[2] pyrkivät edistämään tietoturvallista käyttäytymistä vetoamalla tällaisen käyttäytymisen tuomiin hyötyihin, kun taas negatiivisesti kehystetyt viestit[3] yrittivät saavuttaa saman painottamalla tietoturvallisen käyttäytymisen laiminlyönnistä seuraavia uhkia. Yksilötason viestit puolestaan yrittivät vaikuttaa kohdeyleisöön vetoamalla häneen henkilökohtaisesti, esimerkiksi sinä-pronominein, kun taas yhteisötason viesteissä puhuteltiin yksilöä osana isompaa yhteisöä. (Anderson & Agarwal 2010, 633)

[2] eng. promotion-focused goal frame, oma suomennos.
[3] eng. prevention-focused goal frame, oma suomennos.

Andersonin ja Agarwalin (2010) tutkimustulokset viittaavat siihen, että tehokkaimmin ihmisten käyttäytymiseen näyttäisivät vaikuttavan positiivisesti kehystetyt viestit.

2.3 Tietoturvakäyttäytyminen ja siihen vaikuttaminen

Tässä alaluvussa käsitellään tietoturvakäyttäytymistä koskevaa tutkimuskirjallisuutta. Luvussa esitellään tietoturvakäyttäytymistä ja sen muuttumista selittäviä eri teorioita, kuten suostuttelua ja pelotetta. Lisäksi käsitellään ympäristön, yhteisön sekä henkilökohtaisten ominaisuuksien merkitystä tietoturvakäyttäytymisen kannalta. Aiheen aikaisempi tutkimus on painottunut organisaatiokontekstiin, mutta tietoturvakäyttäytymistä on tutkittu jonkin verran myös yksityishenkilöiden osalta (ks. esim. Anderson & Agarwal 2010). Ihmisten käyttäytyminen voi luonnollisesti vaihdella sen mukaan, toimiiko hän tietyssä tilanteessa itsellisenä yksilönä ja jonkin yhteisön osana. Yhteisössä vallitsevat sosiaaliset normit ja asenteet voivat vaikuttaa ihmisen käyttäytymiseen, kun hän toimii osana jotakin yhteisöä (Pahnila, Siponen & Mahmood 2007). Kuitenkin ihmisen käyttäytymiseen vaikuttavat tekijät voivat olla samoja eri tilanteissakin. Esimerkiksi ihmisen tietyt henkilökohtaiset ominaisuudet, kuten luonne tai kulttuurinen tausta, pysyvät kutakuinkin muuttumattomina tilanteesta toiseen.

Tietoturvakäyttäytymiseen vaikuttavia tekijöitä ovat muiden muassa henkilökohtaiset tekijät sekä kulttuuri- ja ympäristötekijät (Bada ym. 2019). Esimerkiksi riskin ymmärtäminen voi olla jaettu kulttuurinen kokemus, jolloin kulttuurin vaikutuksesta on hyvä olla selvillä tietoisuutta lisäävää työtä tehdessä (Bada ym. 2019, 5). Lisäksi on esitetty, että ihmisten tietoturvakäyttäytymiseen vaikuttaa myös esimerkiksi heidän suhteensa turvattavaan asiaan, kuten tietokoneeseen tai kotiverkkoon, jolloin asian koettu tärkeys ja läheisyys vaikuttavat asiaa koskevaan käyttäytymiseen (Anderson & Agarwal 2010, 638).

Tämän tutkielman tarkoituksena on lisätä ymmärrystä siitä, minkälaisten viestinnällisten kehysten avulla ihmisiä pyritään motivoimaan tietoturvaa edistäviin toimiin. Tutkielmassa ei ole tarkoituksena mitata tai arvioida, miten hyvin nämä motivoimisen keinot onnistuvat tavoitteessaan, eli minkälaisiin toimiin ihmiset tosiasiassa ryhtyvät, tai jättävät ryhtymättä, viestinnän seurauksena. On kuitenkin pantava merkille, ettei pelkästään ihmisten aikomus tehdä jotakin automaattisesti johda siihen, että hän tosiasiassa myös tekee sen.

2.3.1 Käyttäytymiseen vaikuttaminen ja suostuttelu

Ihmisten käyttäytymistä voidaan pyrkiä muuttamaan useilla eri tavoilla. Bada ym. (2019) ovat jakaneet käyttäytymiseen vaikuttamisen kahteen osa-alueeseen. Ensinnäkin voidaan yrittää vaikuttaa ihmisten tietoiseen ajatteluun. Toisaalta on myös mahdollista muuttaa ihmisten automatisoidumpaa käyttäytymistä, mikä ei ole yhtä vahvasti sidoksissa yksilön tekemiin tietoisiin valintoihin. (Ba-

da ym. 2019, 5) Samanlaisen jaottelun ihmisen käyttäytymiseen vaikuttamisesta ovat esittäneet myös Dolan ym. (2012). He kutsuvat tietoista ajattelua ja siihen vaikuttamista kognitiiviseksi malliksi, sekä automaattista toimintaa ja siihen vaikuttamista kontekstimalliksi (Dolan ym. 2012, 265). Dolan ym. (2012) ovat mallintaneet ihmisten käyttäytymiseen vaikuttamista MINDSPACE-mallilla, jonka osa-alueet ovat viestin välittäjä, kannustimet, normit, oletusarvot, huomattavuus, pohjustus, tunteminen, sitoutuminen ja ego[4].

Viestin välittäjällä tutkijat viittaavat siihen, että ihmiset arvottavat tietoa joko positiivisesti tai negatiivisesti riippuen siitä, kuka tai mikä taho on tiedon lähde (Dolan ym. 2012, 266). Ihmisten toimintaan vaikuttaa näin ollen heidän asennoitumisensa tiedon lähteeseen, eli ei ole yhdentekevää, kuka tai mikä taho tietoa välittää. Ihmisten reagoiminen kannustimiin riippuu tutkijoiden mukaan esimerkiksi niiden ajoituksesta, voimakkuudesta ja tyypistä (Dolan ym. 2012, 267). Yhteisössä vallitsevat sosiaaliset ja kulttuuriset normit vaikuttavat niin ikään ihmisten käyttäytymiseen. Se, miten muut ihmiset käyttäytyvät, voi näin ollen olla merkityksellistä yksilön käyttäytymisen muovautumisessa. Tutkijoiden mukaan haluttuja normeja tulisi edistää lisäämällä tietoisuutta niistä esimerkiksi kampanjoiden avulla. (Dolan ym. 2012, 268) Oletusarvoissa puolestaan on kyse siitä, että monissa päätöksentekotilanteissa on tarjolla jonkinlainen oletusarvoinen ratkaisu, jonka voimaanastuminen ei vaadi aktiivista päätöksentekoa. Asettamalla tiettyjä oletusarvoja voidaan vaikuttaa ihmisten käyttäytymiseen, koska ihmisillä on usein tapana noudattaa annettua oletusarvoa (Dolan ym. 2012, 269).

Huomattavuudella tutkijat viittaavat siihen, mikä merkitys jonkin aiheen tai teeman näkyvyydellä ja ihmisten huomion kiinnittämisellä siihen on käyttäytymiseen. Ihmisten huomiota voidaan pyrkiä joko tietoisesti kiinnittämään tiettyihin aiheisiin, tai jokin aihe voi nousta ihmisten huomioon jonkin ulkoisen tapahtuman myötä. On hyvä huomioida, etteivät ihmiset pysty ottamaan asioita huomioon päätöksenteossaan, jos he eivät ole tietoisia niistä. (Dolan ym. 2012, 269) Pohjustus on puolestaan tärkeää, koska se mahdollistaa uuden tiedon omaksumisen. Pohjustuksen on arvioitu olevan tietoisuudesta erillinen prosessi, jonka avulla ihmiset pystyvät paremmin tulkitsemaan ja reagoimaan heille annettuihin uusiin viesteihin. (Dolan ym. 2012, 270) Tunteminen eli tunteiden kokeminen viittaa siihen, miten tunteet vaikuttavat ihmisten käyttäytymiseen ja päätöksentekoon, kun taas sitoutumisella tarkoitetaan ihmisten kykyä sitoutua tietynlaiseen toimintaan. Esimerkiksi ihmisen todennäköisyys sitoutua tietynlaiseen toimintaan kasvaa, jos hän tekee sitoumuksensa julkisesti. (Dolan ym. 2012, 271) Lopuksi egolla tarkoitetaan ihmisten taipumusta toimia niin, että se tukee hänen positiivista omakuvaansa

Furnell ja Rajendran (2012) esittävät mallin, joka pyrkii havainnollistamaan, mitkä tekijät vaikuttavat käytännön tietoturvakäyttäytymiseen. Mallissa huomioidaan sekä henkilön työtä, organisaatiota ja työhön liittyvää vuorovaikutusta koskevat tekijät että henkilön ominaisuuksia koskevat tekijät, kuten

[4] eng. samassa järjestyksessä messenger, incentives, norms, defaults, salience, priming, affect, commitment, ego. Oma suomennos.

laajempi tietoisuus, arvioidut hyödyt ja käytännön kokemukset (Furnell & Rajedran 2012, 13). Kaikkien edellä mainittujen tekijöiden vaikutusten nähdään lisäksi vielä heijastuvan käytäntöön henkilön persoonan kautta (Furnell & Rajedran 2012, 14).

Yksilön käyttäytymiseen voidaan pyrkiä vaikuttamaan esimerkiksi suostuttelevin tekniikoin[5]. Niihin lukeutuvat pelkoon, huumoriin, asiantuntemukseen, toistoon, intensiteettiin ja tieteelliseen näyttöön perustuvat tekniikat. Tutkimusten mukaan ihmiset toimivat usein sen mukaan, miten he käsittävät omat valmiutensa toimia vaaditulla tavalla. (Bada ym. 2019, 5) Esimerkiksi, jos ihminen kokee, että annetut ohjeet ovat liian vaikeaselkoisia ja siten niiden noudattaminen liian vaivalloista, tai ettei hänellä ole tarvittavaa osaamista niiden noudattamiseksi, hän saattaa suuremmalla todennäköisyydellä jättää noudattamatta näitä ohjeita.

Tehdessään käyttäytymistä koskevia päätöksiä ihminen arvioi toiminnasta koituvia hyötyjä ja haittoja (LaRose, Rifon & Enbody 2008, 73). Ihmisten päätöksiin voidaan näin ollen LaRose ym. (2008, 73) mukaan pyrkiä vaikuttamaan korostamalla tietoturvallisen toiminnan positiivisia seurauksia. LaRose ym. (2008, 74) huomauttavat myös, että ihmiset toimivat tietoturvallisesti sitä todennäköisemmin, mitä merkityksellisemmäksi he aiheen itselleen kokevat. Näin ollen ihmisten käyttäytymiseen voitaisiin yrittää vaikuttaa pyrkimällä lisäämään ihmisten kokemusta tietoturvan merkityksestä heille itselleen.

2.3.2 Ympäristö, yhteisö ja vastuun kokeminen

Yhteisöllisissä ympäristöissä, esimerkiksi töissä tai koulussa, ihmisten käyttäytyminen voi linkittyä myös kyseisessä yhteisössä vallitseviin sosiaalisiin normeihin ja asenneilmapiiriin (ks. esim. Pahnila, Siponen & Mahmood 2007). Yksityishenkilöillä ei välttämättä ole vastaavaa ympäristöstä tulevaa painetta toimia tietyllä tavalla, vaikka on luonnollisesti huomioitava, että kukaan yksityishenkilökään tuskin pystyy elämään ympäröivän yhteiskunnan normeista ja toimintatapojen malleista vapaana. Anderson ja Agarwal (2010, 628) tutkimustulokset tukevat ajatusta, että yksityishenkilöiden tietoturvakäyttäytymiseen vaikuttaa myös se, minkälaista toimintaa ihminen ajattelee muiden häneltä odottavan.

LaRose ym. (2008, 74) havaitsivat tutkimuksessaan, että yksilön kokema vastuu vaikutti myönteisesti siihen, kuinka todennäköisesti hän suorittaa tietoturvaa edistäviä toimenpiteitä, kun taas vastaavasti vähemmän henkilökohtaista vastuuta kokeneet eivät toimineet yhtä aktiivisesti. Näin ollen ihminen pyrkisi toimimaan tietoturvaa edistävällä tavalla erityisesti silloin, kun hän kokee olevansa itse henkilökohtaisesti vastuussa tietoturvastaan (LaRose ym. 2008, 74). Tutkijat ehdottavatkin, että tietoturvallisempaa käyttäytymistä voitaisiin pyrkiä edistämään korostamalla henkilön omakohtaista vastuuta, mutta vaarana on se,

[5] eng. persuasive techniques

ettei tämäkään strategia toimi samalla tavalla erilaisille ihmisille, esimerkiksi niille, jotka eivät ole kiinnostuneita tietoturva-asioista (LaRose ym. 2008, 75–76).

Tässä tutkielmassa keskitytään suomalaiseen kulttuuriin, koska kaikki analysoitava materiaali on laadittu suomalaiselle yleisölle. Kulttuuri ja ympäristö ovat kuitenkin merkityksellisiä sen kannalta, minkälaisin keinoin ihmisiin kannattaa yrittää vaikuttaa (Bada ym. 2019, 4), minkä takia asiaa käsitellään tässä yhteydessä lyhyesti. Esimerkiksi uhan tai riskin kokemus voi olla tietyn kulttuurin sisällä jaettu (Bada ym. 2019, 5). Kulttuurit ja yhteiskunnat voivat erota toisistaan esimerkiksi siinä, korostetaanko yhteiskunnassa yksilöllisyyttä vai yhteisöllisyyttä. Individualistisemmissa kulttuureissa ihmiset määrittelevät usein itsensä henkilökohtaisten ominaisuuksiensa mukaan, kun taas yhteisöllisemmissä kulttuureissa ihmisen itsemäärittelyä ohjaa enemmän yksilön asema yhteisössään. Individualismi tai kollektivismi ovat merkittäviä tekijöitä esimerkiksi siinä, mihin tekijöihin kannattaa missäkin kulttuuriympäristössä vedota, jos tavoitteena on vaikuttaa ihmisten käyttäytymiseen. Individualistisemmissa kulttuureissa voi olla kannattavampaa vedota henkilökohtaisiin tekijöihin, esimerkiksi henkilökohtaiseen uhkaan, kun taas yhteisöllisemmissä kulttuureissa yhteisöllisiin tekijöihin, esimerkiksi siihen, miten tietynlainen toiminta voi vahingoittaa yhteisön turvallisuutta. (Bada ym. 2019, 5)

2.3.3 Henkilökohtaiset ominaisuudet

Kuten jo aiemmin mainittiin, niin kutsuttua *one-size-fits-all* -lähestymistapaa ei pidetä kaikkein tehokkaimpana tietoturvatietoisuuden ja halutun tietoturvakäyttäytymisen edistäjänä. Sen sijaan monet tutkimukset puoltavat yksilöiden henkilökohtaisten ominaisuuksien huomioimista tietoturvakoulutuksissa ja -kampanjoissa (ks. esim. Korpela 2015 tai Furnell & Rajendran 2012). Henkilökohtaisiin ominaisuuksiin voidaan lukea esimerkiksi henkilön sukupuoli, ikä tai persoonallisuus. Ihmisen persoonallisuus on merkittävää muun muassa sen kannalta, miten helppoa tai vaikeaa hänen käyttäytymiseensä on vaikuttaa (Furnell & Rajendran 2012, 14), sekä sen kannalta, miten ja minkälaisin keinoin häneen kannattaa yrittää vaikuttaa (ks. esim. Bada ym. 2019). Henkilön persoonallisuuden on todettu vaikuttavan esimerkiksi tietotekniikkaan liittyviin pelkoihin ja huoliin, ja sitä kautta henkilön käyttäytymisaikeisiin (Korzaan & Boswell 2008, 21).

Henkilökohtaisten ominaisuuksien vaikutuksia ihmisten tietoturvakäyttäytymiseen on tarkasteltu monista eri lähtökohdista. Esimerkiksi Gratian, Bandi, Cukier, Dykstra ja Ginther (2018) tarkastelivat tutkimuksessaan demografisten tekijöiden, persoonallisuuden, päätöksentekotapojen sekä riskinoton merkitystä eri tietoturvakäyttäytymisen osa-alueisiin. Tutkijat havaitsivat, että tietyt persoonallisuuden piirteet, erityisesti tunnollisuus, vaikuttivat positiivisesti aikomukseen käyttäytyä tietoturvallisemmin (Gratian ym. 2018, 351–352). Persoonallisuuden lisäksi demografisista tekijöistä erityisesti sukupuoli vaikuttaa tutkimuksen mukaan tietoturvakäyttäytymiseen. Naisten havaittiin noudatta-

van tietoturvakäyttäytymisen normeja heikommin kuin miesten. Lisäksi tiettyjen riskinottotyylien sekä päätöksentekotapojen havaittiin olevan yhteyksissä tietoturvalliseen käyttäytymiseen. (Gratian ym. 2018, 351–352) Gratian ym. (2018, 352) ehdottavatkin henkilökohtaisten ominaisuuksien huomioimista tietoturvakoulutuksissa ja tietoturvakampanjoissa parhaiden mahdollisten tulosten saavuttamiseksi. Toisin sanoen, kampanjat voisivat paremmin vaikuttaa ihmisten käyttäytymiseen, jos ne vetoaisivat juuri yksilön merkittäviksi ja tärkeiksi kokemiin asioihin ja teemoihin.

Myös Kajzer ym. (2014, 69) pitivät tutkimuksessaan erityisesti persoonallisuuden huomioon ottavia viestejä tehokkaina tietoturvakäyttäytymiseen vaikuttamisen keinoina. Tietynlaiset viestit toimivat paremmin tietynlaisia persoonallisuuden piirteitä omaaville ihmisille. Tämä toimii tutkijoiden mukaan myös toisin päin: tietynlaiset viestit voivat vaikuttaa tiettyjä persoonallisuuden piirteitä omaaviin ihmisiin jopa negatiivisesti. (Kajzer ym. 2014, 69)

2.3.4 Pelote

Peloteteoria[6] on tietoturvakäyttäytymisestä koskevassa tutkimuksessa paljon hyödynnetty teoria, joka pyrkii selittämään, miten ihmisten käyttäytymiseen voidaan yrittää vaikuttaa erilaisten pelotteiden ja sanktioiden avulla (Siponen & Vance 2010, 488). Peloteteoriaa on käytetty perinteisesti selittämään erityisesti ihmisten normien, lakien tai sääntöjen vastaista käyttäytymistä (Siponen & Vance 2010, 491). Peloteteoriassa ajatellaan, että päätöksiä tehdessään ihmiset punnitsevat sääntöjen noudattamista tai rikkomista mahdollisesti seuraavia hyötyjä ja kustannuksia, joiden perusteella he päättävät, kumpi toimintatapa on kannattavampi. Peloteteorian mukaan ihmisten käyttäytymiseen vaikuttaa ensinnäkin se, millä todennäköisyydellä hän jää kiinni normin rikkomisesta (*certainty of sanctions*) sekä se, miten ankara rangaistus on tiedossa (*severity of sanctions*) kiinni jäätäessä. (Siponen & Vance 2010, 491) Yksityishenkilöistä puhuttaessa on hyvä pohtia erityisesti näiden kahden tekijän merkitystä käyttäytymiseen vaikuttavana tekijänä. Koska yksityishenkilöt eivät ole tiettyjen tietoturvaohjeiden tai -politiikkojen piirissä, ei heidän toimintaansa valvo kukaan, joten voidaan perustellusti kysyä, kenelle yksityishenkilöt voisivat ylipäätään jäädä kiinni esimerkiksi salasanasuositusten rikkomisesta? Toisaalta samoista syistä myöskään suositusten seuraamatta jättämisestä ei ole tiedossa sanktioita yksityishenkilöille.

Pelotteiksi voidaan peloteteorian eri sovelluksissa määritellä erilainen skaala asioita. Tietoturvakäyttäytymistä koskevissa tutkimuksissa pelotteiksi on määritelty esimerkiksi viralliset sanktiot ja epäviralliset sanktiot, joihin on laskettu kuuluvaksi monipuolisesti erilaisia asioita muiden paheksunnasta henkilökohtaiseen häpeän tunteeseen (Siponen & Vance 2010, 491). Joissain tutkimuksissa häpeän on tulkittu olevan jopa epävirallisista sanktioista erillinen,

[6] eng. deterrence theory, yleisesti käytetty suomennos.

oma pelotteen muotonsa (ks. esim. Paternoster & Simpson 1996). Pelotteen toimivuuden edellytyksenä on, että ihmiset, joiden käyttäytymiseen pelotteen avulla pyritään vaikuttamaan, ovat tietoisia säännöistä ja toivotuista käyttäytymismalleista (Straub 1990, 258). Näin ollen pelotteet on siis kommunikoitava kohdeyleisölle tehokkaasti. Vakuuttavaan pelotteiden käyttämiseen onkin ajateltu liittyvän sallittuun ja haluttuun käyttäytymiseen ohjaamista aktiivisella tiedottamisella sekä kouluttamisella (Straub 1990, 258). Straubin (1990, 272) mukaan tehokkaita pelotetta hyödyntäviä keinoja tietoturvan tapauksessa ovat esimerkiksi erilaisten menetelmien hyödyntäminen haluttua tietoturvakäyttäytymistä ja sen vastaisia toimia koskevassa tiedonlevityksessä, sekä halutun käyttäytymisen vastaisia toimia seuraavista rangaistuksista tiedottaminen. Straubin näkemys on, että organisaatioiden kontekstissa esimerkiksi tietoturvaohjeiden ja -politiikkojen pitäisi olla tarpeeksi yksityiskohtaisia ja selkeitä, jolloin ne lisäisivät tietoisuutta pelotteesta. Lisäksi organisaatioissa pitäisi panostaa halutunlaisen käyttäytymisen tiedottamisesta sekä kouluttamisesta jäsenille. (Straub 1990, 272)

Erilaisia pelotteita asettamalla voidaan pyrkiä saamaan ihmiset käyttäytymään halutulla tavalla. Ihmisten tietoturvakäyttäytymiseen voidaankin yrittää vaikuttaa pelotteilla ja sanktioilla, jotka seuraisivat epätoivottua tietoturvakäyttäytymistä. Toiminnan tarkoituksena on ohjailla ihmisiä välttelemään näitä sanktioita noudattamalla tietoturvasta annettuja ohjeita. Tällainen ohjailu voisi tulla kyseeseen esimerkiksi organisaatioiden kontekstissa, jossa organisaatiossa määriteltyjen tietoturvasääntöjen ja -ohjeiden voidaan ajatella sitovan organisaation jäseniä. Yksityishenkilöitä eivät kuitenkaan sido mitkään tietyt tietoturvakäyttäytymistä koskevat säännöt, eikä esimerkiksi salasanaturvallisuuden laiminlyönnistä ole määritelty yksityishenkilöille sanktioita. Peloteteoriaa ei tästä syystä pidetäkään yksityishenkilöiden kontekstiin täysin soveltuvana teoriana (Li & Siponen 2011, 7). Toisaalta voidaan pohtia, saattaisiko esimerkiksi edellä mainittu häpeä toimia myös yksityishenkilöiden viiteryhmässä käyttäytymiseen vaikuttavana pelotteena.

2.4 Suojelumotivaatioteoria

Tämän alaluvun tarkoituksena on esitellä suojelumotivaatioteoria, eli toinen tutkielman pohjana olevista teorioista. Luvussa perehdytään teoriaa koskevaan aikaisempaan kirjallisuuteen sekä siihen, miten teoriaa on aikaisemmin hyödynnetty tietoturva-alan tutkimuksessa. Suojelumotivaatioteoria on valikoitunut toiseksi tutkielman teorioista, koska se soveltuu hyvin viestinnällisten ja markkinointisisältöjen analysointiin. Uhkia ja niiden herättämiä pelkoja on pyritty käyttämään hyväksi esimerkiksi markkinoinnissa, jossa pelon tunteen herättämistä on hyödynnetty käyttäytymiseen vaikuttamiseksi (Tanner, Hunt & Eppright 1991, 36). Lisäksi suojelumotivaatioteoriaa on käsitelty paljon tietoturvakäyttäytymisen tutkimuksessa, mikä lisää sen mielekkyyttä tämän tutkielman kontekstissa.

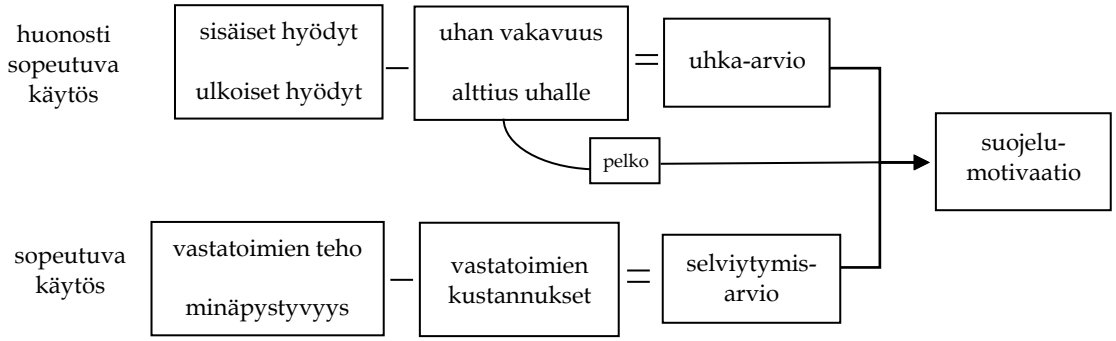
Tietoturvakäyttäytymistä koskevassa tutkimuskirjallisuudessa ihmisten käyttäytymistä on usein pyritty selittämään suojelumotivaatioteorialla[7] (ks. esim. Anderson & Agarwal 2010). Suojelumotivaatioteoriaa on hyödynnetty tietoturva-alan tutkimuksessa erityisesti siksi, koska tietoturvauhat ja niitä vastaan esitetyt suojautumistoimet ovat niin helppo yhdistää. Esimerkiksi käyttäjätilien luvatonta käyttöä ja identiteettivarkauksia voidaan ehkäistä käyttämällä vahvoja ja ainutlaatuisia salasanoja. (Menard & Crossler 2017, 1207) Suojelumotivaatioteoriaa on hyödynnetty erityisesti tilanteissa, joissa on tutkittu, miten hyvin ihmiset päätyvät noudattamaan suostuttelevan viestinnän tarjoamia ohjeita ja suosituksia (Floyd, Prentice-Dunn & Rogers 2000, 411). Toisaalta on myös esitetty, että ihmisten motivoiminen tietoturvatoimiin vetoamalla uhkiin ei välttämättä toimi joka tilanteessa, sillä ihmisillä voi olla suurempi motivaatio suojella esimerkiksi omia tietojaan tai laitteitaan kuin toteuttaa muita, yleisluontoisempia tietoturvatoimenpiteitä (Menard & Crossler 2017, 1207). Kuitenkin suojelumotivaatioteorian soveltamisen kannalta olennaista on mielletty olevan, että tilanteeseen liittyy koettu uhka sekä siihen tarjottu vastatoimi, jonka ihminen voi itse toteuttaa (Floyd ym. 2000, 409). Suojelumotivaatioteoriaa onkin näin ollen käytetty selittämään, miksi ihmisten asenteet ja käyttäytyminen muuttuvat, kun he kohtaavat uhkia (Floyd ym. 2000, 420).

Suojelumotivaatioteoria on kehittynyt alun perin terveysalan teoriana, jolla pyrittiin selittämään, miten ihmisiä voitaisiin motivoida terveyttä edistävään toimintaan (ks. esim. Floyd ym. 2000). Teorian varhaisessa vaiheessa se keskittyi pelkovetoomusten vaikutuksiin terveyskäyttäytymiseen ja -asenteisiin (Rogers 1975). Pelkoon vetoavalla viestinnällä onkin arvioitu aikaansaavan muutosta ihmisten käyttäytymisessä (Floyd ym. 2000, 409). Suojelumotivaatioteoriassa ajatuksena on, että ihmisten toimintaan vaikuttaa heidän kokemansa uhka (Rogers 1975). Suojelumotivaation mallissa huomioidaan niin sisäiset kuin ulkoiset tiedon lähteet. Toimintaan voi näin ollen vaikuttaa sekä ihmisen sisäiset lähteet, kuten aikaisempi kokemus ja saatu palaute, sekä ulkoiset toimijat, kuten muilta oppiminen tai viestinnän vastaanottaminen. (Floyd ym. 2000, 409–410) Ihmisen käyttäytymiseen vaikuttavan suojelumotivaation mallin muodostavat sekä uhan että vastakeinojen arviointi yhdessä (Floyd ym. 2000, 410).

Suojelumotivaatioteoria tunnistaa kolme tekijää, joiden avulla voidaan ymmärtää, miten ihmiset kokevat ja arvioivat uhkia (ks. esim. Vance, Siponen & Pahnila 2012, 190). Nämä ovat epätoivottavasta käyttäytymisestä seuraavat hyödyt ja palkinnot, uhan vakavuus sekä ihmisen alttius kyseiselle uhalle. Jos epätoivottavasta käyttäytymisestä on luvassa hyötyjä tai palkintoja, lisää se todennäköisyyttä toimia epätoivottavalla tavalla (Floyd ym. 2000, 410). Vastaavasti jos ihminen mieltää uhan vakavaksi, hän todennäköisemmin tarttuu vastatoimiin uhkaa vastaan (Floyd ym. 2000, 410). Lisäksi suojelumotivaatioteoriassa on tunnistettu niin ikään kolme tekijää, jotka vaikuttavat ihmisen kykyyn selviytyä uhasta. Näihin lukeutuvat usko vastatoimien tehoon uhkaa vastaan, vastatoimien kustannukset sekä minäpystyvyys eli usko siihen, että vastatoimet ovat toteutettavissa (Vance ym. 2012, 190) Suojelumotivaatioteorian mallia ha-

[7] eng. protection motivation theory (PMT)

vainnollistetaan kuviossa 1. Toimintaan ryhtymisen tai käyttäytymisen muuttamisen taustalla on myös ajatus siitä, että ihmisen tulisi kokea uhkaa vastaan esitettyjen toimien olevan tarpeeksi tehokkaita ja hänen toteutettavissaan (Anderson & Agarwal 2010, 628). Näin ollen ihmisille ehdotettavat käyttäytymistavat ja toimintatavat pitäisi olla ihmisen taitoihin suhteutettuja, jotta ihminen voi kokea pystyvänsä suorittamaan hänelle ehdotetut tarvittavat toimenpiteet. Ihminen, joka omaa positiivisen asenteen ehdotettuja toimia kohtaan, toimii todennäköisemmin myös ohjeiden mukaan, kuin jos hän olisi vain peloissaan (Anderson & Agarwal 2010, 628).



KUVIO 1: Suojelumotivaatiomalli (mukaillen Floyd ym. 2000, 410)

Näin ollen toiminnan, kuten viestinnän, jonka tarkoituksena on saada ihmiset toimimaan tietoturvallisemmin, tulisi vedota uhan vakavuuteen ja ihmisen alttiuteen tälle uhalle. Uhkien vakavuuden ja alttiuden korostaminen saattaa johtaa kohdeyleisössä pelon syntymiseen, mutta pelon ei saa antaa lamauttaa kohdeyleisöä. Sen takia onkin tärkeää, että viestinnän, tai muun tietoturvallisempaan käyttäytymiseen motivoivan toiminnan, tulisi luoda kohdeyleisössä uskoa ehdotettujen vastatoimien tehoon sekä ihmisen kykyyn toteuttaa näitä vastatoimia. Suojelumotivaatioteorian kontekstissa viestinnän onnistumisen tai tehokkuuden mittarina voidaankin pitää sen kykyä saada kohdeyleisössä syntymään aikomus hyväksyä viestinnän esittämä ehdotus (Floyd ym. 2000, 421). Viestinnän esittämänä ehdotuksena voidaan ymmärtää esimerkiksi viesti uhan vakavuudesta, kohdeyleisön alttiudesta uhalle tai uhkaa vastaan esitetyt vastatoimet. Luonnollisesti on hyvä tiedostaa, että pelkkä aikomus toimia tietyllä tavalla ei välttämättä suoraan johda aiottuun toimintaan (Floyd ym. 2000, 421).

Jotta ihminen päätyisi uhan kokiessaan vastatoimiin sen sijaan, että toimisi epätoivottavalla tavalla, hänen tulee uskoa, että uhka on olemassa, ja että hän on uhalle altis (Floyd ym. 2000, 420). Lisäksi näiden käsitysten uhan olemassaolosta sekä kyseisen henkilön omasta alttiudesta sille on ohitettava painoarvossaan epätoivottavasta käyttäytymisestä seuraavien palkintojen ja hyötyjen houkutus. Ihmisen on myös uskottava, että ehdotetut vastatoimet ovat tehokkaita, edullisia sekä hänen toteutettavissaan, jotta hän päätyisi luopumaan epätoivottavasta käyttäytymisestä ja tarttuisi vastatoimiin. (Floyd ym. 2000, 420) Floyd ym. (2000, 420) havaitsivat metatutkimuksessaan, että vastakeinojen arviointi

näyttäisi olevan vähän vahvemmassa yhteydessä toivottuun käyttäytymiseen kuin uhan arviointi, vaikka molempien yhteys toivottuun käyttäytymiseen oli havaittavissa.

Ihmisten aikomukseen toimia tietoturvallisesti voi vaikuttaa esimerkiksi motivaatio (Menard & Crossler 2017, 1208). Menardin ja Crosslerin (2017, 1223) mukaan ihmisen motivaatio tietoturvatoimia kohtaan ei kuitenkaan ole yhtä ilmeistä kuin motivaatio suojeleviin toimiin esimerkiksi oman terveyden kontekstissa, eikä aina ole selvää, mitkä tekijät motivaatioon vaikuttavat. Merkillepantavaa on, että samaa uhkaa vastaan esitetyt eri vastatoimet aiheuttavat erilaisia kustannuksia tai menetyksiä, jolloin toinen vastatoimi voi vaikuttaa houkuttelevammalta kuin toinen. Samoin sama vastatoimi voidaan kokea tehokkaammaksi yhtä uhkaa vastaan kuin toista, mikä viestijän kannattaa ottaa huomioon pohtiessaan, mihin asioihin on missäkin yhteydessä kannattavaa viitata. (Floyd ym. 2000, 422) On myös hyvä huomioida, ettei suojelumotivaatioteoria oleta päätöstä tekevän ihmisen olevan rationaalinen toimija (Floyd ym. 2000, 420). Ihmisten voi olla joissain tilanteissa vaikea arvioida tietyn toiminnan mahdollisia lopputuloksia, jolloin myös käyttäytymisen ennakoiminen voi olla haastavaa (Floyd ym. 2000, 420–421).

Suojelumotivaatioteoriaa on kritisoitu esimerkiksi siitä, ettei se huomioi tarpeeksi pelkovetoomuksien aikaansaamia tunnereaktioita (Tanner ym. 1991, 37). Tanner ym. (1991, 37–38) huomauttavat, että Rogersin alkuperäinen suojelumotivaatioteorian malli ei kiinnitä tarpeeksi huomiotta pelkoon, vaan keskittyy sen sijaan vain kognitiivisiin tekijöihin. Heidän näkemyksensä mukaan suojelumotivaatioteoriaa voitaisiin kehittää tunnistamalla tunneperäisten prosessien merkitys uhkia koskevien kognitiivisten arvioiden tekemisessä, jolloin tunteet voivat näin ollen vaikuttaa arvion tekemistä seuraavaan käyttäytymiseen (Tanner ym. 1991, 38).

2.5 Sosiaalinen markkinointi

Tässä alaluvussa esitellään sosiaalisen markkinoinnin teoriaa. Luvussa käydään läpi teorian taustaa sekä esitellään sen aikaisempaa hyödyntämistä tutkimuksessa. Sosiaalinen markkinointi on valittu mukaan tähän tutkielmaan, koska se tarjoaa uudenlaisen näkökulman tietoturvatietoisuuden lisäämiseen ja tietoturvaviestintään yksityishenkilöiden kontekstissa. Huomionarvoista on, ettei tutkielman aineisto välttämättä edusta tietoisesti laadittua sosiaalista markkinointia, mutta aineistossa voi silti esiintyä tiedostamattomia sosiaalisen markkinoinnin piirteitä, minkä takia sosiaalisen markkinoinnin näkökulma on tutkimuksessa perusteltu. Tutkielman tarkoituksena on ylipäätään luoda parempaa ymmärrystä siitä, miten sosiaalinen markkinointi soveltuu tietoturvan kontekstiin, ja minkälaisia mahdollisuuksia sekä keinoja sosiaalinen markkinointi voisi tietoturvaviestintään jatkossa tarjota.

Kuten tässä työssä on jo aiemmin useampaan otteeseen mainittu, tietoturva koskettaa jatkuvasti enemmän kaikkia kansalaisia, mutta kansalaisten tietoi-

suus tietoturvauhista tai tietoturvallisesta käyttäytymisestä ei kehity itsestään. Voidaan kuitenkin argumentoida, että tietoturvan merkitys kasvaa ja tulee yhä edelleen kasvamaan siinä määrin, että yhteiskunnan tietoturvan takaamiseksi tarvitaan laajoja toimia eri yhteiskunnan toimijoilta. Kansalaisten tietoturvatietoisuus ja -käyttäytyminen ovat merkittäviä tekijöitä yhteiskunnan tietoturvan kannalta, esimerkiksi koska niin moni nyky-yhteiskunnan palveluista on Internetissä. Kansalaisten tietoturvatietoisuutta pitäisi näin ollen pyrkiä kehittämään, ja sosiaalisen markkinoinnin menetelmät voisivat olla tässä yhteydessä avuksi. Sosiaalinen markkinointi sopii aihealueen tutkimukseen, koska voidaan ajatella, että digitalisaation myötä lisääntynyt tarve myös tietoturvaosaamiselle on merkittävä yhteiskunnallinen ilmiö, joka vaatii kansalaisten käyttäytymisen ja asenteiden muutosta, johon voitaisiin pyrkiä sosiaalisen markkinoinnin keinoin.

Sosiaalisella markkinoinnilla tarkoitetaan markkinoinnin keinovalikoimien hyödyntämistä yhteiskunnallisten ongelmien ratkaisemiseen (Lefebvre 2013, 4). Sosiaalisesta markkinoinnista on yleensä puhuttu esimerkiksi köyhyyden poistamiseen, terveyden edistämiseen sekä ympäristöasioihin liittyvissä yhteyksissä. Sosiaalisen markkinoinnin juuret ovat yritysmarkkinoinnissa, ja se on kehittynyt tarpeesta saavuttaa laajempaa muutosta yhteiskunnassa. Sosiaalisen markkinoinnin teorian tarkoitus on tarjota työkaluja haastavien ja laajojen ongelmien ratkaisemiseksi. (Lefebvre 2013, 4–5) Perinteinen markkinointi voidaan ymmärtää yritysten pyrkimyksinä saada ihmiset ostamaan tuotteita tai palveluja aina uudelleen, asioimaan yrityksen kanssa, kuuntelemaan yrityksen viestejä sekä jakamaan niitä eteenpäin (Hastings 2007, 3). Siinä missä tavallinen yritysmarkkinointi keskittyy ihmisten kulutuskäyttäytymiseen, kuten jonkin tuotteen tai palvelun ostamiseen, sosiaalinen markkinointi on enemmän kiinnostunut laajemmista kokonaisuuksista, kuten tämän kulutuskäyttäytymisen laajemmista vaikutuksista. Esimerkiksi kuluttajan päätöstä ostaa tupakkatuotteita voidaan tarkastella ostokäyttäytymistä laajemmin terveydellisenä käyttäytymisenä. (Hastings 2007, 4)

Sosiaalinen markkinointi on hitaasti eriytynyt yritysmarkkinoinnista noin 1960–luvulta lähtien, kun tutkijat kiinnostuivat markkinoinnin hyödyntämismahdollisuuksista kaupallisen toiminnan ulkopuolella. Nykyisin sosiaalista markkinointia pidetään omana markkinoinnin osa-alueenaan. Sosiaalisen markkinoinnin muotoutumiseen ovat lisäksi vaikuttaneet erityisesti terveyden edistämisen ja yhteiskunnallisen muutoksen käytännön harjoittajat, joiden ideoimat kampanjat ja muut toimenpiteet ovat osaltaan muovanneet alaa omanlaisekseen. (Lefebvre 2013, 16)

Rothschildin (1999, 24) mukaan ihmisten käyttäytymiseen vaikuttaminen markkinoinnin keinoin edellyttää jonkinlaista vaihtokauppaa tai vastavuoroisuutta. Jos ihminen on tyytyväinen nykyiseen käyttäytymiseensä, täytyy sen muuttamiseksi tehdä jonkinlainen vaihtokauppa, jossa ihminen kokee saavansa jotain vastineeksi käyttäytymisensä muuttamisesta. Rothschild huomauttaa, että ihmisten käyttäytymiseen vaikuttamisessa laeilla, kouluttamisella ja markkinoinnilla on kaikilla oma paikkansa ja roolinsa. (Rothschild 1999, 24) Rothschild erottaa koulutuksen ja markkinoinnin toisistaan kuvaamalla koulutuksen

tiedottamiseksi tai kohdeyleisön taivuttamiseksi tietynlaiseen toimintaan ilman vastavuoroisuutta, eli tarjoamatta palkintoja tai rangaistuksia (Rothschild 1999, 25). Koulutuskin kyllä monesti lupaa kohdeyleisölle erilaisia hyötyjä, kuten kannustamalla terveellisen ruuan syöntiin lupaamalla terveyshyötyjä, mutta ajatus vaihtokaupasta ei ole läsnä samoin kuin markkinoinnissa. Tosin markkinoinninkin on haastavampaa hyödyntää vaihtokauppaa, kun kyseessä on yhteiskunnallinen asia, kuten terveyskäyttäytyminen. Tämä johtuu siitä, että näissä tilanteissa luvatut palkinnot ovat usein saavutettavissa vasta pitkän ajan kuluttua, jos silloinkaan. Ylipäätään vaihtokauppaan liittyy tällaisissa tapauksissa epävarmuus. (Rothschild 1999, 26–27) Tietoturva näyttäytyy niin ikään haastavana markkinoitavana, koska sen tarjoama vaihtokauppa, turvallisuus, voi vaikuttaa kohdeyleisön mielestä hyvin abstraktilta. Lisäksi, jos ihminen ei tunnista itseensä kohdistuvaa uhkaa, tai pidä sitä varteenotettavana, voi turvallisuuden tarjoaminen vaihtokauppana näyttäytyä ihmisen silmissä tarpeettomalta ja houkuttelemattomalta. Tällöin ihmistä voi olla hyvin vaikea motivoida tietoturvaa edistävään käyttäytymiseen.

Rothschild (1999, 28) huomauttaa myös, ettei sosiaalisen markkinoinnin kontekstikaan ole kilpailusta vapaa. Yritysmarkkinoilla yritykset kilpailevat keskenään, mutta sosiaalisen markkinoinnin kentällä kilpailu muodostuu vallitsevien asenteiden ja käytösmallien sekä haluttujen tavoiteasenteiden sekä -käytösmallien välille (Rothschild 1999, 28). Artikkelissaan Rothschild esittää MOA-mallin hyödyntämistä sosiaalisessa markkinoinnissa. MOA-malli muodostuu englanninkielisistä motivaatiota, mahdollisuutta ja kykyä tarkoittavista sanoista[8]. MOA-mallissa ihmisen käyttäytyminen ja sen muutos voi tapahtua, jos ihmisellä on motivaatiota, mahdollisuus ja kyky toteuttaa käyttäytymistä. Käyttäytyäkseen tietyllä tavalla ihmisellä pitää olla motivaatio, joko ulkoinen tai sisäinen, toimia niin. Myös sosiaalisten olosuhteiden ja resurssien on oltava kunnossa, että käyttäytyminen on mahdollista. Lisäksi ihmisen pitää omata tarvittavat tiedot ja taidot käyttäytymisen toteuttamiseksi. (Rothschild 1999, 31–32)

Dahl, Eagle & Ebrahimjee (2013, 238) huomauttavat, että onnistuakseen sosiaalisen markkinoinnin kampanjan on otettava huomioon käyttäytymisen taustalla vaikuttavat motivaatiotekijät. Prochaska ja DiClemente (1982) pyrkivät selittämään ihmisten terveyskäyttäytymisen muutosta transteoreettisella mallilla[9]. Malli perustuu ajatukseen, että käyttäytymisen muutos tapahtuu vaiheittain. Ensimmäinen vaihe on esitutkiskelu, jossa ihminen ei vielä aio muuttaa käyttäytymistään. Seuraava vaihe on tutkiskelu, jossa ihmisellä on jo todellinen aikomus muuttaa käyttäytymistään, mutta hän ei ole vielä tehnyt käytännön sitoumuksia muutoksen eteen. Tätä seuraa valmisteluvaihe, jossa käyttäytymisen muutos on jo lähellä, ja ihminen on jo tehnyt jotain pieniä asioita käyttäytymisen muuttamiseksi. Neljännessä vaiheessa, toimintavaiheessa, ihminen on jo onnistuneesti muuttanut käytöstään, mutta muutos on vielä suhteellisen tuore. Lopulta ylläpitovaiheen saavuttaneen ihmisen käyttäytymisen muutos on pysynyt voimassa jo useita kuukausia. (Sarkin, Johnson, Prochaska & Prochaska

[8] eng. motivation, opportunity, ability, oma suomennos.

[9] eng. the transtheoretical model (TTM)

2001, 462–463) Erityisesti ensimmäiseen, mutta myös toiseen vaiheeseen liittyy usein epätietoisuus aiheesta, jolloin tietoisuuden lisääminen linkittyy vahvasti näihin vaiheisiin (Dahl, Eagle & Ebrahimjee 2013, 237). Mallia on hyödynnetty sosiaalisen markkinoinnin tutkimuksessa esimerkiksi senioriväestön liikuntakäyttäytymiseen vaikuttamisen kontekstissa (Dahl ym. 2013).

Sosiaalisen markkinoinnin suunnittelussa ja toteutuksessa voidaan hyödyntää apuna myös Rogersin (2003) esittämää ajatusta innovaatioiden diffuusiosta. Teoksessaan Rogers määrittelee diffuusion omanlaisekseen viestinnän muodoksi, jossa pyritään saamaan jokin uusi innovaatio leviämään yhteiskunnassa. Diffuusio on näin ollen prosessi, jossa uudesta ideasta viestitään eri kanavissa ajan saatossa yhteiskunnan jäsenten kesken. Rogers pitää diffuusiota myös eräänlaisena sosiaalisen tai yhteiskunnallisen muutoksen ajurina. Diffuusiota tapahtuu, kun uusia ajatuksia syntyy, ne leviävät ja ne joko hyväksytään tai torjutaan, mikä johtaa erilaisiin muutoksiin. (Rogers 2003) Innovaatioiden omaksujat voidaan jakaa luokkiin sen mukaan, miten nopeasti ja ennakkoluulottomasti he omaksuvat uudet ideat ja innovaatiot. Kaikkein innokkaimpia omaksujia ovat innovoijat, joiden jälkeen tulevat järjestyksessä varhaiset omaksujat ja varhainen enemmistö. Näitä hitaammin uudet ideat vastaanottavat myöhäinen enemmistö, ja kaikkein hitaimmin hitaat omaksujat. (Rogers 2003) Nämä luokittelut voivat olla hyödyllisiä sosiaalisen markkinoinnin keinovalikoimaa ja kohderyhmä suunnitellessa. Eri kohderyhmien vakuuttamiseksi voidaan tarvita eri keinovalikoimia, ja eri kohderyhmille kannattaa suunnata erilaisia viestejä. Kuten aikaisemmin mainittu Rothschild esitti, sosiaalinen markkinointi on vain yksi mahdollinen keino vaikuttaa ihmisten käyttäytymiseen; myös laeilla ja kouluttamisella voidaan saada aikaan muutoksia käyttäytymisessä (Rothschild 1999, 24). Joihinkin tilanteisiin ja joillekin kohdeyleisöille ne sopivat jopa sosiaalista markkinointia paremmin (Rothschild 1999, 24).

Lefebvre esitteli teoksessaan *Social marketing and social change: strategies and tools for health, well-being, and the environment* (2013, 50–52) kahden osatekijän muodostaman viitekehyksen sosiaaliselle markkinoinnille. Nämä kaksi osatekijää ovat ihmiskeskeisyys sekä kokonaisvaltaiseen muutokseen pyrkiminen prioriteettisegmenttien avulla. Sosiaalisessa markkinoinnissa, niin kuin markkinoinnissa muutenkin, ihminen ja se, mitä hän haluaa tai tarvitsee, on keskiössä. Sosiaalisen markkinoinnin harjoittajan on lisäksi hyvä huomioida, että ihmisellä on oikeus valinnanvapauteen. Tarkoituksena ei myöskään Lefebvren mukaan ole kohdentaa viestejä yksilöille, vaan tunnistaa muutoksen kannalta tärkeimmät segmentit eli ryhmät, joille sosiaalisen markkinoinnin viestit tulisi suunnata, ja sitä kautta pyrkiä laajempaan yhteiskunnalliseen muutokseen. Sosiaalisen markkinoinnin kampanjoiden tulisi näin ollen hyödyntää malleja ja teorioita, jotka käsittelevät käyttäytymistä ja sen muutosta laajemmin kuin yksilötasolla. (Lefebvre 2013, 50–52)

Näiden kahden osatekijän pohjalta Lefebvre on muodostanut neljä toimenpidettä, joiden tarkoituksena on auttaa sosiaalisen markkinoinnin tekijää tunnistamaan prioriteettisegmentit sekä se, minkälaista arvoa ja hyötyä juuri heille tulisi tarjota. Näihin toimenpiteisiin kuuluvat prioriteettiryhmän tunnis-

taminen, sekä prioriteettiryhmän toiveiden ja tarpeiden ymmärtäminen. Näiden kahden lisäksi pitää ymmärtää, mitkä tekijät saavat prioriteettiryhmän käyttäytymään tavalla, jolla he nyt käyttäytyvät, ja jota sosiaalisella markkinoinnilla yritetään muuttaa, ja miten näitä tekijöitä voitaisiin pyrkiä muuttamaan. Neljäs toimenpide on sosiaalisen markkinoinnin kampanjan muotoilu haluttuun prioriteettiryhmään vetoavaksi, jolloin kampanjan tulisi tarjota kyseiselle kohderyhmälle hyötyä tai arvoa tuovia vaihtoehtoja. (Lefebvre 2013, 52–53)

Sosiaalista markkinointia on kritisoitu muun muassa manipulatiiviseksi (Lefebvre 2013, 45), ja uhria syyllistäväksi keinovalikoimaksi (Lefebvre 2013, 22). Lefebvre (2013, 49) arvostelee sosiaalisen markkinoinnin harjoittajia alalla ajoittain vallitsevasta liiasta keskittymisestä yksilön käyttäytymiseen. Hän muistuttaakin, että sosiaalisessa markkinoinnissa tavoitteena tulisi yksilön käyttäytymisen muuttamisen sijaan olla laajempi yhteiskunnallinen muutos (Lefebvre 2013, 49). Sosiaalisen markkinoinnin yhteydessä voidaan käydä myös eettistä pohdintaa, onhan koko konseptin ajatuksena vaikuttaa ihmisten käyttäytymiseen. Miten voidaan taata, että vaikuttaminen tapahtuu eettisten periaatteiden mukaan, eikä sosiaalisen markkinoinnin käyttö aiheuta haittaa tai vaaraa yksilöille tai yhteiskunnalle? Sosiaalisen markkinoinnin tarkoitus on edistää yhteiskunnallista hyvää, mutta voidaan kysyä, mitä yhteiskunnallinen hyvä ylipäätään on ja kuka sen saa määritellä (Lefebvre 2013, 70). Lefebvren aikaisemmin esiteltyihin prioriteettiryhmien valintaan sisältyy myös arvovalintoja. Miksi juuri kyseinen ryhmä on valittu prioriteettiasemaan, ja miten valinta vaikuttaa kyseiseen ryhmään (Lefebvre 2013, 70)? Sosiaalisen markkinoinnin harjoittajien tulisi myös kunnioittaa ihmisten itsemääräämisoikeutta, eikä haluttuja arvoja tai käyttäytymistä saa pakottaa (Lefebvre 2013, 71). Sosiaalinen markkinointi on luonteensa takia kiinteästi yhteydessä yhteiskunnallisiin epäkohtiin, kuten ihmisten väliseen eriarvoisuuteen, koska se käsittelee ongelmia kuten köyhyys ja terveys. Sosiaalisen markkinoinnin harjoittajien on näin ollen syytä pohtia tarkasti käyttämiään keinoja, etteivät ne lisää eriarvoisuutta tai ihmisten kokemaa stigmaa (Lefebvre 2013, 70–71).

2.6 Yhteenveto

Tässä luvussa esiteltiin tutkielman teoreettinen viitekehys. Kuten luvussa kävi ilmi, yksityishenkilöiden tietoturvan tutkimuksessa on havaittu, että yksityishenkilöt kokevat olevansa oman onnensa nojassa tietoturva-asioissa. Jos yksityishenkilöiden ajatellaan olevan vastuussa tietoturvastaan, heitä pitäisi tutkijoiden mukaan opastaa paremmin, ja heidän tietoisuuttaan tietoturva-aiheista pitäisi pyrkiä lisäämään. (Furnell ym. 2007)

Tietoturvaviestintää puolestaan on tutkittu paljon erityisesti kampanjoiden näkökulmasta. Kampanjoita on tarkasteltu esimerkiksi viestin välittämisen keinojen näkökulmasta, jolloin erityisesti video- ja tekstiperustaiset keinot miellyttivät yleisöä (Abawajy 2014). Tietoturvakampanjoiden kompastuskiveksi muodostuvat tutkimuksen mukaan niiden epämääräiset ja liian monimutkaiset

ohjeistukset sekä pelon lietsonta (Bada ym. 2019). Näiden lisäksi erityisesti niin kutsutun *one-size-fits-all* -mallin hyödyntäminen on tutkimusten mukaan kampanjoiden heikkous. Sen sijaan, että kaikille suunnattaisiin samanlaista sisältöä, tutkijat pitävät tärkeänä, että kampanjamateriaalit suunnitellaan kohderyhmälle sopiviksi. Lisäksi materiaalien tulisi huomioida ihmisten henkilökohtaisia ominaisuuksia sekä kulttuurista tai muuta taustaa. (Kajzer ym. 2014, Bada ym. 2019)

Tietoturvakäyttäytymistä ja siihen vaikuttamista käsittelevää tutkimuskirjallisuutta esiteltiin teoreettisen viitekehyksen puitteissa esimerkiksi suostuttelun ja pelotteen käsitteiden kautta. Ihmisten käyttäytyminen todettiin olevan useiden tekijöiden summa, eikä siihen vaikuttaminenkaan tapahdu täysin yksiselitteisesti. Tutkijat ovat kuitenkin havainneet, että esimerkiksi ihmisten tekemät arviot tietyn käyttäytymisen hyödyistä ja haitoista voivat vaikuttaa käyttäytymiseen (LaRose ym. 2008).

Tässä tutkielmassa analyysi nojaa kahteen eri teoriaan: ihmisten käyttäytymistä selittävään suojelumotivaatioteoriaan sekä sosiaaliseen markkinointiin. Suojelumotivaatioteorian mukaan ihmiset arvioivat uhkia sen perusteella, mikä on uhan vakavuus, mikä on ihmisen alttius uhalle, sekä mitä hyötyjä tai palkintoja voi seurata, jos jatkaa käyttäytymistä tietyllä tavalla uhasta huolimatta (Vance ym. 2012). Teorian mukaan ihmisten kykyyn selviytyä uhasta vaikuttavat usko vastatoimien tehoon, vastatoimien kustannukset, sekä usko, että vastatoimet ovat ihmisen toteutettavissa (Vance ym. 2012). Sosiaalisen markkinoinnin kannalta olennaisena pidetään tutkijoiden mukaan vaihtokaupan tai vastavuoroisuuden ajatusta, jonka mukaan sosiaalisen markkinoinnin viestien tulisi tarjota ihmiselle jotain vastineeksi käyttäytymisen muuttamisesta (Rothschild 1999). Lefebvren (2013) esittelemän viitekehyksen mukaan sosiaalisessa markkinoinnissa on kaksi olennaista osatekijää: ihmiskeskeisyys ja kokonaisvaltaiseen muutokseen pyrkiminen prioriteettisegmenttien avulla.

3 TUTKIMUSASETELMA

Tässä luvussa esitellään tutkielman tutkimusasetelma, johon lukeutuu selostus tutkielman toteuttamisesta, tutkimuksessa käytettävän menetelmän esittely sekä tutkimusaineiston esittely. Ensimmäisessä alaluvussa esitellään tutkielman aineisto, joka koostuu Kyberturvallisuuskeskuksen yksityishenkilöille tuottamista tietoturvaviestinnän materiaaleista. Tämän jälkeen kuvaillaan tutkimuksen menetelmää eli kehysanalyysia, ja lopulta käydään läpi tutkielman varsinainen toteutus.

3.1 Aineisto

Tutkielman aineisto muodostuu yksityishenkilöille suunnatuista tietoturvaviestinnän materiaaleista. Aineistoon on valittu mukaan suomalaisen julkaisijan tuottamia suomenkielisiä materiaaleja. Valtaosa aineistosta on tekstipohjaista, mutta mukaan on valittu myös kolme Kyberturvallisuuskeskuksen julkaisemaa lyhyttä videota, joiden litteraatit löytyvät tämän tutkielman lopusta liitteestä 2. Koska tutkimus käsittelee nimenomaan yksityishenkilöille suunnattua tietoturvaviestintää, aineistoa valitessa olennaista oli sen kohderyhmä. Mukaan analyysiin on valittu vain niitä aineistoja, jotka ovat selvästi kohdistettu yksityishenkilöille, jolloin aineiston ulkopuolelle jätettiin ne tarjolla olleet materiaalit, jotka ovat suunnattu esimerkiksi tietoturva-asiantuntijoille tai organisaatioiden ja yritysten jäsenille.

Aineisto valikoitiin Kyberturvallisuuskeskuksen tuottamista viestinnällisistä materiaaleista. Kyberturvallisuuskeskus valikoitui aineiston lähteeksi, koska sillä voidaan ajatella valtiollisena tietoturvatoimijana olevan merkittävä asema tietoturvaa koskevassa viestinnässä. Erityisesti yksityishenkilöiden näkökulmasta Kyberturvallisuuskeskus saattaa näyttäytyä yhtenä harvoista toimijoista, jotka tarjoavat myös tavallisille kansalaisille kohdennettua tietoturvaviestintää, ja joka toimii heille tietoturvaa koskevan asiantuntijatiedon lähteenä.

Aineistoa valittiin Kyberturvallisuuskeskuksen verkkosivuilta kategoriasta *Ohjeet ja oppaat yksityishenkilöille*, sekä Traficomin, jonka alaisuudessa Kyberturvallisuuskeskus toimii, YouTube-kanavalta, josta mukaan valikoitui kolme *Kotiturvalistit*-sarjan videota. Videot valittiin mukaan, koska ne sopivat sarjan nimen perusteella oivallisesti mukaan analyysiin. Lisäksi aineiston haussa käytettiin Kyberturvallisuuskeskuksen ajankohtaisten tietoturvauutisten *Tietoturva Nyt!* -palstaa, joka sisälsi hakuhetkellä yhteensä 194 artikkelia. Nämä kaikki käytiin läpi ja niistä valittiin analyysiin mukaan ne, jotka oli selkeästi suunnattu yksityishenkilöille. *Tietoturva Nyt!* -artikkelien joukossa oli paljon erilaisia ohjeita ja neuvoja ajankohtaisia tietoturvauhkia vastaan, mutta näitä artikkeleja ei valittu mukaan, koska ne keskittyivät pääasiassa kuvaamaan ilmiöitä ja kertomaan miten suojautua, jolloin niissä ei olisi juurikaan analysoitavaa. Sen sijaan mukaan valikoitui yleisempiä artikkeleja, kuten kaikki saatavilla olevat 10 tietoturvanäkymää tulevalle vuodelle -artikkelit, top tietoturvauhat ja ratkaisut -artikkelit, vuosien 2019 ja 2020 Tietoturvan vuosi -katsauksien esipuheet, sekä kaksi tietoturvakuukauden alkamisesta kertovaa tiedotetta. Nämä valitut *Tietoturva Nyt!* -artikkelit soveltuivat analysoitavaksi niin oikean kohderyhmänsä kuin tietoturvasta yleisellä tasolla puhumisen takia. Yhteensä aineistoon valikoitui seitsemän Ohjeet ja oppaat -kategorian tekstiä, kolme videota sekä 17 *Tietoturva Nyt!* -artikkelia.

On mielekästä, että aineistossa on mukana ohjeiden ja oppaiden lisäksi myös arkisia tiedotteita, Tietoturvan vuosi -katsauksen pääkirjoituksia sekä tulevia tietoturvauhkia ennakoivia artikkeleita, koska nämä mahdollistavat laajemman kuvan muodostumisen siitä, miten Kyberturvallisuuskeskus viestii tietoturvasta, ja miten tietoturvasta erilaisissa yhteyksissä puhutaan. Esimerkiksi arkisemmat tiedotteet tuotetaan yleensä nopeammin, jolloin niistä voi ilmetä erityisesti tiedostamattomia kehyksiä. Mukaan valitut aineistot, joita on yhteensä 27 kappaletta, löytyvät luettelona liitteestä 1.

Lisäksi on hyvä huomioida, että vaikka toinen tutkielmassa hyödynnettävä teoria on sosiaalinen markkinointi, niin itse aineisto ei välttämättä ole alun perin laadittu sosiaalisen markkinoinnin periaatteet huomioiden. Näin ollen on mahdollista, että aineisto ei edusta tietoisesti suunniteltua sosiaalista markkinointia. Sosiaalisen markkinoinnin teoria soveltuu silti tutkielman kontekstiin, koska sen periaatteita voi ilmetä aineistossa myös ilman, että sitä olisi tietoisesti suunniteltu. Tutkielman aineisto pystyy joka tapauksessa tarjoamaan viitteitä siitä, miten sosiaalisesta markkinointia voisi hyödyntää tietoturvaviestinnässä jatkossa, mitä sen harjoittamisessa tulisi tietoturvan kontekstissa ottaa huomioon, ja mitä mahdollisuuksia siinä piilee.

3.2 Kehysanalyysi

Kehysanalyysi on sosiologi Erving Goffmanin kehittämä menetelmä, joka soveltuu erityisesti viestinnällisten aineistojen tutkimukseen. Kehysanalyysin perusteoksena pidetään Goffmanin vuonna 1974 ilmestynyttä teosta *Frame Analysis:*

An Essay on the Organization of Experience. Teoksessaan Goffman (1986, 1) määrittelee kehystämisen eräänlaiseksi tilanteen määrittelyksi. Kehystämistä voidaan näin ollen hyödyntää vastaamaan kysymykseen ”mitä tilanteessa on meneillään?”[10] (Goffman 1986, 8). Tilanteiden määrittelyllä tarkoitetaan prosessia, jossa ihminen johonkin tilanteeseen päädyttyään joutuu arvioimaan tilannetta sekä pohtimaan, mitä kyseisessä tilanteessa on meneillään, minkälaisia toimintatapoja tilanteessa on tarjolla, ja mitä niistä ihmisen tulisi tilanteessa hyödyntää (Goffman 1986, 1–2). Kehystäminen ei kuitenkaan ole Goffmanin mukaan täysin objektiivinen, vaan enemmänkin henkilökohtainen prosessi, sillä sama tilanne voi aikaansaada erilaisia tulkintoja riippuen siitä, kuka tulkitsee. Tulkintoihin vaikuttavat niin ihmisten erilaiset henkilökohtaiset ominaisuudet kuin taustatkin. (Goffman 1986, 8)

Kuten Goffmanin teoksen nimestä voi päätellä, kehysanalyysi tunnetaan englanniksi nimellä Frame analysis. Englannin kielen sana ’frame’ onkin kehysanalyysin yhteydessä suomennettu sanaksi ’kehys’. Karvonen (2000, 78) pohtii artikkelissaan vaihtoehtoisia suomennoksia sanalle, ja luettelee esimerkkeinä sanoja kuten kehikko, runko, puitteet ja raamit. MOT-sanakirja tarjoaa sanalle ’frame’ suomennokseksi kehyksen lisäksi muiden muassa sanoja karmi, runko, kehikko, puitteet ja tausta. Karvosen (2000, 78) mukaan suomenkielisessä tutkimuskirjallisuudessa kehys on jo vakiintunut suomennos. Hän pitää suomennosta kuitenkin ongelmallisena sen luomien mielleyhtymien takia, koska kehys johtaa Karvosen mielestä suomalaisen ajatukset liikaa maalauksen kehyksiin. Tätä Karvonen pitää harhaanjohtavana lähtökohtana, koska kehysten vaihtaminen maalauksen ympärillä ei muuta kuitenkaan itse maalausta, kun taas kehysanalyysissa ajatuksena on nimenomaan asioiden kehysten kautta saamat merkitykset. Karvonen itse pitää parempana terminä mielleyhtymien kannalta esimerkiksi sanoja runko ja ranko, joista käy ilmi niiden perustavanlaatuinen merkitys lopputuloksen kannalta. Esimerkiksi talot voivat olla ulkoisesti hyvinkin erilaisia riippuen siitä, minkälainen runko siihen rakennetaan. (Karvonen 2000, 78)

Karvosen (2000, 83) mukaan kehyksen käsite on jossain määrin rinnastettavissa esimerkiksi diskurssin käsitteeseen. Näillä kahdella termillä on kuitenkin eriävät lähtökohdat. Diskurssi-termin tausta on kuitenkin enemmän kielitieteessä ja semiotiikassa, kun taas kehys perustuu muiden muassa fenomenologiseen, retoriseen ja sosiaalisen kognition tutkimukseen. (Karvonen 2000, 83) Karvonen erottelee kehyksen ja diskurssin toisistaan kuvaamalla diskurssia luonteeltaan digitaaliseksi ja kehystä analogiseksi, koska diskurssit perustuvat siihen, miten ne eroavat toisistaan, kun taas kehyksissä olennaista on hahmojen tunnistaminen. Kehysten maailmassa merkittävää on tilanteiden tulkinta, ja diskursseissa sosiaaliset käytännöt. (Karvonen 2000, 84)

Joissain tilanteissa tulkinnat ovat helpompia, mutta joitain tilanteita voi tulkita useilla eri tavoilla, jolloin tulkitsija etsii vihjeitä siitä, mikä on oikea tulkinta juuri siinä tilanteessa (Karvonen 2000, 79). Asiantuntijoilla on auktoriteettiasemansa ansiosta Karvosen mukaan merkittävä rooli tilanteiden tulkinnassa,

[10] eng. ”*What is it that is going on here?*” oma suomennos.

ja yhteiskunnassa käydään loputonta kamppailua siitä, kenen tulkinta tilanteesta nousee hallitsevaksi (Karvonen 2000, 80). Tässä tutkielmassa näkökulmana onkin juuri asiantuntijoiden tekemä kehystäminen, jossa tarkoituksena voidaan tulkita olevan Karvosen kuvauksen mukaisesti yrittää saada omalle kehystykselle lisää näkyvyyttä ja saavuttaa vallitseva asema muihin kehyksiin nähden. Ihmisen voi olla haastavampaa perustella itselleen hallitsevan kehyksen ohittamista omassa toiminnassaan, mikä tukisi näkemystä siitä, että viestintämateriaalien tuottajat pyrkisivät lisäämään kehyksensä merkittävyyttä.

Robert Entman (1993) määrittelee kehystämisen seuraavasti:

> Kehystäminen on sitä, että valitaan jotain näkökulmia hahmotetusta todellisuudesta ja tehdään ne näkyvämmiksi viestinnällisessä tekstissä sellaisella tavalla, joka edistää tiettyä ongelman määritelmää, kausaalista tulkintaa, moraalista arviointia ja/tai ehdotettua ongelman käsittelyä.[11] (Entman 1993, 52)

Kehysanalyysissa on näin ollen kyse tilanteiden tulkinnoista, jotka muodostavat kehyksiä. Kehys on siis tulkinta siitä, mikä tilanteessa on merkittävää, ja mikä sitä määrittelee. Tällöin kyseessä on eräänlainen valintaprosessi, jossa joitain tekijöitä korostetaan samalla kun joitain muita häivytetään tai jätetään vaille huomiota. (Karvonen 2000, 82) Valinta voi syntyä joko tietoisesti tai tiedostamatta (Karvonen 2000, 82), minkä takia kehysten tutkiminen on mielekästä. Kehysten tunnistaminen voi auttaa viestijää ymmärtämään, minkälaista kuvaa hän todellisuudesta rakentaa, ja pohtimaan, onko kuva muodostunut tarkoituksellisesti. Jos viestijä ei tiedosta kehyksiä, hän ei välttämättä onnistu luomaan tehokkaasti haluamaansa kuvaa todellisuudesta, jolloin viestin vastaanottajakin voi haparoida yrittäessään saada selvää siitä, mikä on viestijän kuvaama todellisuus.

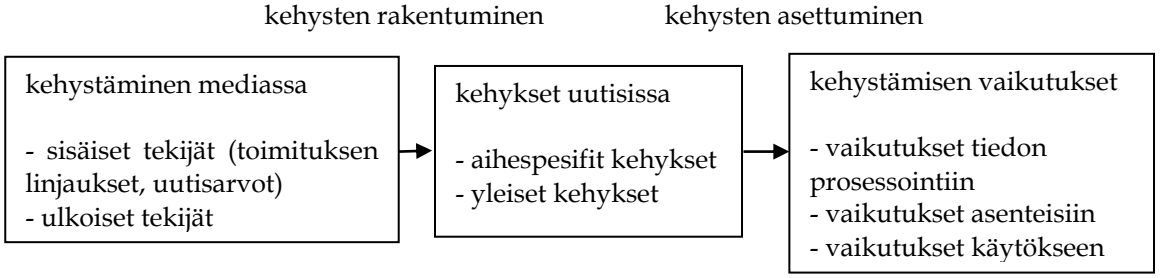
De Vreese (2005, 53) puolestaan määrittelee kehystämisen prosessiksi, jossa nostetaan näkyväksi ja korostetaan aiheen eri puolia. De Vreese nimeää kaksi eri tapaa tunnistaa kehyksiä tekstistä. Ensimmäinen näistä on induktiivinen, jossa kehykset muotoutuvat aineistoa analysoidessa. Toinen tapa on deduktiivinen, jossa kehykset on määritelty etukäteen, ennen aineistoon perehtymistä. (De Vreese 2005, 53) Toinen mahdollinen kehysten luokittelu on jakaa kehykset aihespesifeihin ja yleisiin kehyksiin[12] (De Vreese 2005, Ikäheimo 2016). Aihespesifit kehykset linkittyvät tiettyihin aiheisiin, eikä niitä esiinny muiden aiheiden parissa, kun taas yleiset kehykset voivat olla universaaleja, aiheesta riippumattomia (De Vreese 2005, 54 & Ikäheimo 2016, 271). De Vreese jakaa kehystämisprosessin kahteen osaan, kehysten rakentumiseen sekä asettumiseen[13]. Rakentumisella viitataan kehysten muotoutumisprosessiin ja siihen vaikuttaviin tekijöihin, kun taas asettumisella tarkoitetaan valmiiden kehysten vuoro-

[11] eng. ”To frame is to select some aspects of a perceived reality and make them more salient in a communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation for the item described.” (Entman 1993, 52) Oma suomennos.

[12] eng. issue-spesific frames, generic frames. Suomennos Ikäheimo 2016.

[13] eng. frame-building, frame-setting. Oma suomennos.

vaikutusta kohdeyleisön asenteiden ja ennakkotietojen kanssa. (De Vreese 2005, 52) De Vreesen näkemystä kehysten muotoutumisprosessista esitellään kuviossa 2.



KUVIO 2: Kehysten muotoutumisprosessi (mukaillen De Vreese 2005, 52)

Kehysanalyysin heikkoutena voidaan pitää sen varsin subjektiivista luonnetta, mikä johtuu siitä, että kehysanalyyttinen tutkimus perustuu usein tutkijan omiin tulkintoihin (Ikäheimo 2016, 270). Ongelmallisiksi muotoutuvat erityisesti kehysanalyyttisten tutkimusten toistettavuus ja yleistettävyys, samoin kuin tutkijoiden määrittelemien kehysten erottaminen median itse muodostamista kehyksistä. Kehysanalyysi kärsiikin jossain määrin teoreettisesta hajaannuksesta, mikä on johtanut siihen, että kehysanalyysi on hyödynnetty varsin eri tavoin erilaisissa tutkimuksissa. (Ikäheimo 2016, 270)

Heikkouksistaan huolimatta kehysanalyysilla on paikkansa laadullisessa tutkimuksessa. Tämän tutkielman yhteyteen kehysanalyysi soveltuu, koska analysoitava aineisto on viestinnällistä, mikä on omiaan kehysanalyyttisille tutkimuksille. Lisäksi kehyksiä on sivuttu jo aikaisemminkin tietoturvaa koskevassa tutkimuksessa, kuten alaluvusta 2.2.3 saatiin huomata, jolloin tämä analyysi rakentaa aikaisemman tutkimuksen varaan, ja jatkaa tietoturvaviestinnän kehysanalyyttista tutkimusta. Kehysanalyysi auttaa ymmärtämään, miten tietoturvasta viestitään eri yleisöille, tämän tutkielman kontekstissa yksityishenkilöille. Se auttaa tunnistamaan viestinnän sävyjä, ja ymmärtämään, minkälaista kuvaa tietoturvasta kohdeyleisölle viestinnän pohjalta muodostuu. Nämä ovat tärkeitä tietoja erityisesti viestinnän tekijöille, jotka voisivat käyttää kehyksiä tietoisesti hyväkseen, kunhan niitä ensin tunnistetaan.

3.3 Tutkimuksen toteutus

Kehysanalyysia koskeva tutkimuskirjallisuus ei anna paljonkaan käytännön viitteitä siihen, miten kehysanalyyttinen tutkimus tulisi tarkalleen toteuttaa. Näin ollen kehysanalyysia on hyödynnetty varsin erilaisissa asetelmissa eri tutkimuksissa. Tämän tutkielman tekemisessä hyödynnetään kasvatustieteilijä Anna-Maija Puroilan vuonna 2002 julkaisemassa väitöskirjassa *Kohtaamisia päiväkotiarjessa – kehysanalyyttinen näkökulma varhaiskasvatustyöhön* esittelemää analyysitapaa. Puroilan lähestymistapa kehysanalyysiin voidaan pitää toimivana, koska se on järjestelmällisesti muotoiltu ja hyvin dokumentoitu, jolloin saman-

laisen tutkimusasetelman rakentaminen on sujuvaa. Perusteellisesti jäsennellyn analyysitavan hyödyntäminen voidaan nähdä myös tutkimuksen validiteettia ja erityisesti reliabiliteettia vahvistavana tekijänä, koska tutkimuksen toistettavuus paranee, kun käytetty analyysitapa on hyvin perusteltu ja johdonmukaisesti suunniteltu sekä kuvattu.

Puroilan (2002, 58) kehysanalyysi jakautuu kolmeen vaiheeseen:

1) tilanteiden ja kielellisten kuvausten jäsentäminen aineistosta analyyttisten viitekehysten avulla
2) löydettyjen tilanteiden ja kielellisten kuvausten luokittelu ja kehysten nimeäminen
3) aineiston läpikäynti uudelleen muodostettujen kehysten lähtökohdista

Ensimmäisessä vaiheessa aineistoa jäsennellään analyyttisin viitekehyksin, jolloin aineistosta etsitään erilaisia tilanteita ja kielellisiä kuvauksia. Toisessa vaiheessa tehtyjä havaintoja luokitellaan etsien niistä samankaltaisuuksia, jolloin varsinaiset kehykset muodostuvat, ja ne voidaan nimetä. Lopulta kolmannessa vaiheessa aineistoa käydään läpi uudelleen muodostuneiden kehysten lähtökohdasta, jolloin kehyksille ominaisia ajatuksia ja toimintaa voidaan eritellä tarkemmin, samoin kuin esitellä kehysten keskinäisiä suhteita. (Puroila 2002, 58)

Kehysanalyysi on valikoitunut tämän tutkielman menetelmäksi, koska se soveltuu hyvin viestinnällisten aineistojen tutkimiseen, johon sitä on aikaisemminkin usein hyödynnetty. Tutkielman tavoitteena on tunnistaa viestinnän sävyjä sekä tapoja, joilla tietoturvasta tavallisille kansalaisille viestitään, ja kehysanalyysi soveltuu luonteensa ansiosta oivallisesti tähän tarkoitukseen. Puroilan kehysanalyysimenetelmä toimii tässä kontekstissa, koska se antaa puitteet tarkastella erityisesti kielellisiä ilmaisuja ja tehdä johtopäätöksiä niiden pohjalta. Toisaalta Puroilan tutkimus eroaa jonkin verran luonteeltaan tästä tutkielmasta, koska Puroila hyödyntää väitöskirjansa aineistona haastatteluja. Tämä tutkielma puolestaan perustuu kirjallisiin viestintämateriaaleihin sekä videoihin. Eroavaisuus ei kuitenkaan muodostu ongelmalliseksi, sillä Puroilan analyysitapa soveltuu myös kirjallisen kielen tarkasteluun.

Kuten jo aikaisemmin johdantoluvussa mainittiin, tutkielman tutkimuskysymys on seuraava: *Miten viestinnällisten kehysten avulla pyritään vaikuttamaan ihmisten tietoturvakäyttäytymiseen yksityishenkilöille suunnatussa tietoturvaviestinnässä?* Näin ollen tarkoituksena tutkielmassa on tunnistaa aineistosta eri viestinnällisiä kehyksiä, sekä pohtia syitä juuri näiden kehysten hyödyntämiseen. Luonnollisesti tämän tutkielman puitteissa ei voida saada tarkkaa tietoa siitä, miksi aineistoon lukeutuvien viestintämateriaalien kehykset ovat juuri sellaisia kuin ne ovat, koska tutkielmassa ei haastatella aineistoon kuuluvia materiaaleja laatineita ihmisiä. Näin ollen ei voida myöskään varmasti sanoa, ovatko kyseiset kehykset muodostuneet tarkoituksella vai tiedostamatta. Tutkimus pyrkii ennemminkin lisäämään tietoisuutta yksityishenkilöille suunnatusta tietoturvaviestinnästä sekä niistä sävyistä ja tyyleistä, joilla tietoturvasta viestitään.

Tämä tutkielma on toteutettu Puroilan kolmivaiheista analyysitapaa mukaillen, kuitenkin pienin eroavaisuuksin. Tässä analyysissa hyödynnettiin

deduktiivista kehysanalyysitapaa, jossa kehyksiä määriteltiin jonkinasteisesti jo ennen analyysin aloittamista. Näin voidaan välttää erityisesti induktiiviseen kehysanalyysiin liittyviä toistettavuuden ja yleistettävyyden puutteita. Muodostamalla kehyksiä etukäteen tutkimusasetelma on helpommin toistettavissa, ja analyysin subjektiivisuutta pyritään minimoimaan. Tämän tutkielman kehykset on muodostettu tutkielman teoreettisen viitekehyksen pohjalta, ja ne esitellään Analyysi-luvun alussa. Siinä missä Puroilan analyysivaihe yksi lähti niin sanotusti puhtaalta pöydältä, tässä tutkielmassa ensimmäisen analyysivaiheen lähtökohtana on tutkielman teoreettinen viitekehys, joka tarjoaa suuntaviivoja siihen, minkälaisia kielellisiä kuvauksia aineistosta lähdettiin etsimään. Puroilan analyysitavassa kehykset muotoutuvat havaintojen luokittelun myötä vasta analyysivaiheessa kaksi, kun taas tässä analyysissa alustavat kehykset muotoiltiin jo ennen analyysia. Vaiheessa kaksi tämän tutkielman kehykset kuitenkin saavuttivat lopullisen muotonsa aineistosta tehtyjen havaintojen luokittelun perusteella. Tämän tutkielman kolmas analyysivaihe on lähtökohdiltaan jo varsin samanlainen Puroilan analyysin kanssa, ja tässäkin tutkielmassa vaiheessa kolme käydään aineistoa uudelleen läpi muodostuneiden kehysten lähtökohdasta.

Näistä tutkimusasetelmien eroista huolimatta Puroilan analyysitapa soveltuu lähtökohdaksi tämän tutkielman kontekstiin, sillä se pohjautuu vahvasti kielellisten ilmaisujen tarkasteluun ja ryhmittelyyn, samoin kuin tämän tutkielman analyysikin. Vaikka kehyksiä on muodostettu jo ennen analyysin alkua, niin aineistosta lähdetään samalla tavalla etsimään kielellisiä kuvauksia, jonka jälkeen niitä ryhmitellään ja luokitellaan, minkä pohjalta vasta lopulliset kehykset muotoutuvat. Toisin sanoen, analyysin alkaessa aineistosta lähdettiin etsimään suojelumotivaatioteoriaan ja sosiaaliseen markkinointiin viittaavia kielellisiä ilmaisuja, ja lopullisen muotonsa samoin kuin nimensä kehykset saivat Puroilan analyysitavan mukaisesti vaiheessa kaksi. Vaikka Puroilan analyysitapaa ei noudateta täysin, se tarjoaa tutkielmalle hyvän lähtökohdan, ja sen hyödyntäminen on perusteltua erityisesti ottaen huomioon, ettei kehysanalyysia koskeva tutkimuskirjallisuus itsessään anna paljonkaan viitteitä siihen, miten kehysanalyysia tulisi tehdä. Puroilan analyysitapa tarjoaakin tälle tutkimukselle analyyttiset raamit, joihin nojata.

4 ANALYYSI

Tämä luku sisältää tutkielman varsinaisen analyysiosion. Kuten aiemmin jo mainittiin, analyysi on toteutettu kehysanalyyttisellä menetelmällä, ja tarkastelun kohteena on Kyberturvallisuuskeskuksen yksityishenkilöille suunnatut viestinnälliset materiaalit. Analyysissa vastataan seuraavaan tutkimuskysymykseen: *miten viestinnällisten kehysten avulla pyritään vaikuttamaan ihmisten tietoturvakäyttäytymiseen yksityishenkilöille suunnatussa tietoturvaviestinnässä?* Analyysiosio alkaa analyysivaiheiden tarkemmalla kuvauksella Puroilan analyysitavan vaiheita yksi ja kaksi mukaillen, sekä kehysten määrällisellä analyysilla. Lopulta siirrytään käsittelemään kehyksiä tarkemmin vaihetta kolme noudattaen.

Kuten aiemmin jo mainittiin, analyysissa tarkasteltavat kehykset muodostettiin alustavasti tutkielman teoreettisen viitekehyksen pohjalta, ja ne saivat lopullisen muotonsa analyysivaiheessa 2. Analyysissa muodostuneet kehykset ovat seuraavat:

1) *Uhkapuheen kehys*
2) *Yhteiskunnallisen ulottuvuuden kehys*

Uhkapuheen kehys liittyy suojelumotivaatioteoriaan. Uhkapuheella voidaan yrittää vaikuttaa siihen, miten kohdeyleisö arvioi uhkaa sekä siihen, miten kohdeyleisö uskoo selviytyvänsä uhasta. Yhteiskunnallisen ulottuvuuden kehys johdetaan puolestaan sosiaalisesta markkinoinnista, ja se jakautuu kahteen erilaiseen puheeseen: vaihtokauppapuhe sekä muutospuhe. Vaihtokauppapuhe tarkoittaa viestejä, joilla tarjotaan sosiaalisen markkinoinnin ytimessä olevaa vaihtokauppaa tai vastavuoroisuutta. Muutospuhe puolestaan viittaa viesteihin, joissa puhutaan muutoksesta tai tietoturvan yhteiskunnallisesta merkityksestä. Tämä liittyy sosiaaliseen markkinointiin, koska sen tarkoituksena on edistää laajaa yhteiskunnallista muutosta.

Kuten aiemmin jo kuvailtiin, analyysi toteutettiin Puroilan kolmivaiheista analyysitapaa mukaillen sillä erotuksella, että analyysia ohjasi teoreettinen viitekehys, johon viittaavia kirjallisia ilmaisuja lähdettiin etsimään aineistoista samalla tavalla luokitellen kuin Puroilan analyysissakin. Tämän tutkielman analyysivaiheet ovat seuraavat:

1) Aineistosta etsitään tutkimuskirjallisuuteen viittaavia kielellisiä kuvauksia
2) Kehykset saavuttavat lopullisen muotonsa aineistosta tehtyjen havaintojen luokittelun perusteella
3) Aineiston läpikäynti muodostuneiden kehysten lähtökohdasta

Analyysivaiheessa yksi aineistoa käytiin läpi etsien suojelumotivaatioteoriaan ja sosiaalisen markkinoinnin teoriaan liittyviä kielellisiä ilmaisuja ja tilanteita. Tässä vaiheessa pohdittiin esimerkiksi, minkälaiset tekijät tekstissä viittaavat suojelumotivaatioteoriaan ja sosiaalisen markkinoinnin teoriaan. Esimerkki tästä analyysivaiheesta ja sen toteutuksesta on nähtävissä taulukosta 1.

Taulukko 1: analyysivaihe 1

Aineisto	Analyyttiset kysymykset	Analyysi ja tulkinta
”*Moneen* internetissä käytettyyn palveluun on kohdistunut *suuria salasanavuotoja.* Jopa miljoonia käyttäjätunnus-salasana-pareja on *vuodettu yleisesti saataville*.”	Mikä on näkökulma ja konteksti?	Kolme ensimmäistä lainausta kuvaavat tietoturvan maailmaa erilaisten uhkien kautta, kun taas kolme jälkimmäistä lainausta kuvaa tietoturvaa muuttuvan maailman tärkeänä kansalaistaitona, ja tarjoaa vastavuoroisuutta.
”Kyberrikollisuudelta ja tietoturvahaavoittuvuuksilta suojautuminen *ei tule helpottumaan*.”	Mitkä tekijät viittaavat suojelumotivaatioon?	Puhutaan moniin palveluihin kohdistuneista valtavista tietovuodoista, tietoturvauhilta suojautumisen vaikeutumisesta ja rikollisten oveluuden lisääntymisestä. Nämä kaikki voidaan tulkita suojelumotivaatiota provosoivina tekijöinä.
”Rikolliset ovat keksineet entistäkin *ovelampia keinoja kalastella tietojasi* erilaisten huijausten avulla.”		
”Omasta *tietoturvasta huolehtiminen on tärkeä taito* digitaalisessa maailmassa.”		
”*Inhimillisen tietoturvan* merkitystä ei saa unohtaa eikä aliarvioida. Kyberturvallisuudesta ei voi tulla *arjen kansalaistaitoa*, jos emme viesti siitä inhimillisesti ja ymmärrettävästi.”	Mitkä tekijät viittaavat sosiaaliseen markkinointiin?	Muutospuhe, inhimillisyys sekä vastavuoroisuus. Tavoitteena on yhteiskunnallinen muutos vaihtokaupan keinoin.
”*Uusi oppaamme kertoo, kuinka voit huolehtia tietoturvastasi* yksinkertaisin keinoin”	Minkälaisia sanoja ja kielellisiä kuvauksia käytetään?	Esimerkeistä on kursivoitu uhkiin, muutospuheeseen sekä vastavuoroisuuteen viittaavia sanoja.

Analyysivaiheessa 2 puolestaan aineistosta löydettyjä ilmaisuja luokiteltiin, ja muodostettiin kehykset. Suojelumotivaatioteorian pohjalta muotoutui uhkapuheen kehys, ja sosiaalisen markkinoinnin teorian pohjalta yhteiskunnallisen ulottuvuuden kehys. Uhkapuheen kehykseen luokiteltiin ilmaisuja, joissa kuvailtiin erilaisia uhkia esimerkiksi uhkien yleisyyden ja uhan realisoituessa vaarantuvien asioiden kautta. Yhteiskunnallisen ulottuvuuden kehykseen luokiteltiin puolestaan ilmaisuja, joissa puhuttiin muutoksesta tai vastavuoroisuudesta. Vastavuoroisuus ilmeni aineistossa usein tavalla, jossa kuvailtiin tietoturvauhkien vaarantamia asioita, ja tarjottiin lukijalle keinoja uhan välttämiseksi. Kuten Taulukosta 1 voidaan huomata, sosiaalisen markkinoinnin kehys voidaan jakaa kahteen erilaiseen osa-alueeseen: toisaalta on muutospuhe, mutta lisäksi myös vaihtokauppaan tai vastavuoroisuuteen viittaava puhe. Analyysivaihetta kaksi on esitelty tarkemmin taulukossa 2. Koska analyysi toteutettiin etsimällä aineistosta valmiiksi määriteltyjä kehyksiä, voi olla mahdollista, että aineistosta olisi voinut löytyä myös jotain muita kehyksiä, jotka nyt jäivät tarkastelun ulkopuolelle.

Taulukko 2: analyysivaihe 2

Kehys	Esimerkkejä kielellisistä ilmaisuista
Uhkapuheen kehys	tietojen/rahan menettäminen, uhkia kaikkialla, uhka koskettaa kaikkia, huijareita missä vaan, voidaan huijata, entistä ovelampia, päästä käsiksi tietoihin, ilmiöt eivät ohimeneviä, huijausviestit vievät rahasi/tietosi, käyttäjää uhkaavat, jotain ikävää tulee tapahtumaan, huijauksilta tuskin vältymme, salauksellakin voidaan huijata, monet palvelut, suuria tietovuotoja
Yhteiskunnallisen ulottuvuuden kehys	ottamalla käyttöön vältät, vaikeutuu entisestään, kestää vielä pitkään, osaamisen saavuttaminen, toimimalla näin pärjäät myös, käytä hyviä salasanoja niin tietosi pysyvät turvassa, arjen kansalaistaito, tuoda tietoturva jokaiseen kotiin, kyberturvallisuus kuuluu kaikille, mä haluan vaan pelata, se on paras tapa pitää hakkerit loitolla

4.1 Kehysten määrällinen analyysi

Kehysten esiintymiä oli löydettävissä aineistosta yhteensä 155, joista 80 lukeutui yhteiskunnallisen ulottuvuuden kehykseen, ja 75 uhkapuheen kehykseen. Tarkasteltavat kaksi kehystä ilmenivät siis aineistossa määrällisesti tasaisesti.

Kehysten esiintymismäärät aineistoja kohtaan on esitelty taulukossa 1. Taulukko on jaettu kahteen kategoriaan, joista ensimmäinen koostuu *Tietoturva Nyt!* -artikkeleista (myöhemmin TTN), ja jälkimmäinen *Ohjeet ja oppaat yksityishenkilöille* -osion teksteistä (myöhemmin Ohjeet ja oppaat). Kategoriat on erotettu toisistaan paksulla mustalla viivalla, ja niiden sisällä aineisto esitetään aikajärjestyksessä vanhimmasta uusimpaan. Videot on tässä yhteydessä luokiteltu osaksi Ohjeet ja oppaat -kategoriaa.

Taulukko 3: kehysten esiintymät aineistossa

Aineiston otsikko	Yhteiskunnallisen ulottuvuuden kehys	Uhkapuheen kehys
TOP 5 tietoturvauhat ja -ratkaisut yksityishenkilöille	1	5
10 + 1 näkymää tietoturvan vuodelle 2019	6	1
Kyberturvallisuus kuuluu kaikille	8	0
Tunnista, suojaudu ja torppaa nettihuijarin aikeet	2	2
Nasevia neuvoja tiliesi turvaamiseksi	0	1
Hallitsetko nämä tietoturvan perustaidot?	3	1
Turvalisti-Teijo on mukana Euroopan kyberturvallisuuskuukaudessa	5	2
Suomi aloittaa älylaitteiden turvallisuuden varmistamisen ensimmäisenä Euroopassa – uusi Tietoturvamerkki auttaa kuluttajia tekemään turvallisempia kodin älylaitehankintoja	8	1
Yhteiskuntamme haavoittuvuuksia ei korjata vain keskustelemalla	3	0
Tietoturvan selviytymispakki koteihin ja toimistoihin – 3 uhkaa ja ratkaisua	4	5
10 tietoturvanäkymää vuodelle 2020	1	5
Yhteiskunta tarvitsee tietoturvallisia arjen tekoja – yhdessä olemme vahvin lenkki	5	2
Neuvoja epäilyttävien sivujen tunnistamiseksi	3	4
#tietoturvatorstai - Ota arjen tietoturva haltuun asiantuntijoidemme kanssa	3	0
Kyberturvallisuuden superkuukausi on täällä taas!	5	0
10 tietoturvanäkymää vuodelle 2021	3	6
Tietoturva 2021: 3 uhkaa ja 3 ratkaisua jokaiselle	4	2
Turvallisuusopas poikkeusolojen jälkeiseen aikaan	4	2
Salasanat haltuun – Kuka käyttää tiliäsi?	4	4
Pidempi parempi – Näin teet hyvän salasanan	0	2
Netiketti – Verkossa liikkujan työkalupakki	0	2
Näin suojaudut tietomurroilta	0	4
Näin suojaudut nettihuijaukselta	0	6
Näin pidät huolta tietoturvasta kotona ja työpaikalla	3	9
Kotiturvalistit – Äly-TV (video)	2	3
Kotiturvalistit – Salasana (video)	1	3
Kotiturvalistit – Päivitykset (video)	2	3
Yhteensä	**80**	**75**

Kuten taulukosta 1 käy ilmi, eri kehykset jakautuvat aineistossa varsin tasaisesti. Kaikki aineistot on julkaistu vuosina 2019, 2020 ja 2021, joten ajallinen tarkastelu ajoittuu vain vähän yli kahden vuoden ajanjaksolle. Tämä johtuu siitä, ettei Kyberturvallisuuskeskuksen verkkosivuilla ollut saatavilla vanhempia materiaaleja. Kehyksiä esiintyykin ajallisesti tarkasteltuna varsin tasaisesti, eikä kolmen vuoden aikana ole tapahtunut aineiston perusteella merkittävää muutosta siinä, miten kehyksiä esiintyy. Kuten jo mainittiin, kehyksiä esiintyy lukumäärällisesti myös varsin tasaväkinen määrä. Havaittavissa oli kuitenkin jonkin verran eroja sen suhteen, minkälaisissa aineistoissa kumpaakin kehystä esiintyi enemmän, ja joissain aineistoissa ilmeni vain jompaa kumpaa kehystä. Yhteiskunnallisen ulottuvuuden kehystä ilmeni aineistossa eniten, mutta toisaalta aineistoja, joissa sitä ei ilmennyt ollenkaan, oli enemmän kuin aineistoja, joissa ei esiintynyt ollenkaan uhkapuheen kehystä, sillä yhteiskunnallinen kehys jäi nollille viidessä aineistossa, kun taas uhkapuheen kehystä ei esiintynyt ollenkaan neljässä aineistossa. Erot kehysten esiintymisten yhteismäärien välillä ovat kokonaisuudessaan kuitenkin pieniä, ja johtuvat tarkasteltavien materiaalien luonteiden eroista ja erityyppisten materiaalien pituuseroista.

Aineistossa on kuitenkin havaittavissa tiettyä erikoistumista, koska yhteiskunnallista puhetta esiintyy huomattavasti uhkapuhetta enemmän, jos tarkastellaan vain TTN-artikkeleja. TTN-artikkeleissa uhkapuheen kehystä esiintyy 37 kertaa, kun taas yhteiskunnallisen ulottuvuuden kehystä jopa 64 kertaa. Toisaalta uhkapuheen kehys esiintyy tasaisesti, sillä Ohjeet ja oppaat -osiossa sitä ilmenee 38 kertaa. Yhteiskunnallisen ulottuvuuden kehys onkin huomattavasti epätasaisemmin jakautunut, koska sitä esiintyy Ohjeet ja oppaat -osiossa vain 16 kertaa. Näin ollen eri kehysten esiintymien väliset erot ovat suuret molempien kategorioiden sisällä, minkä lisäksi yhteiskunnallisen ulottuvuuden kehyksen sisällä on suurta vaihtelua sen mukaan, mihin kategoriaan tarkasteltu aineisto lukeutuu.

Nämä erot kertovat ensinnäkin siitä, että TTN-artikkelit ja Ohjeet ja oppaat -osion materiaalit ovat sisällöllisesti erilaisia. Uhkapuhetta esiintyy molemmissa varsin tasaisesti, mutta yhteiskunnallista puhetta esiintyy selvästi enemmän TTN-artikkeleissa, koska ne ovat luonteeltaan erilaisia kuin Ohjeet ja oppaat -osion materiaalit. Siinä missä Ohjeet ja oppaat -osion aineistot pyrkivät nimensä mukaisesti neuvomaan ja opastamaan, TTN-artikkelien joukkoon lukeutuu myös paljon yleisluoteisempia tekstejä, joissa keskitytään tietoturvaan nimenomaan yhteiskunnallisesta näkökulmasta. Nämä artikkelit voivat olla tyyliltään kantaaottavia, tai muuten tietoturvasta yleisemmällä tasolla kertovia, kun taas Ohjeet ja oppaat -osion materiaalit usein ohittavat kokonaan tietoturvan yhteiskunnallisen merkityksen. Kantaaottavuutensa ja tietoturvan yhteiskunnalliseen merkitykseen keskittymisensä vuoksi vaikuttaa luontevalta, että yhteiskunnallisen ulottuvuuden kehystä esiintyy juuri TTN-artikkelien joukossa enemmän. Uhkapuheen tarkoituksena voidaan puolestaan tulkita olevan vaikuttaa ihmisten käyttäytymiseen, kuten suojelumotivaatioteoriakin ehdottaa, mikä vaikuttanee siihen, miksi uhkapuhetta ilmenee enemmän nimenomaan Ohjeet ja op-

paat -osion materiaaleissa, onhan niiden tarkoituksena juuri ohjeistaa tietynlaiseen tietoturvakäyttäytymiseen.

Eniten kehysten yhteenlaskettuja esiintymiä löytyi Ohjeet ja oppaat -osion tekstistä *Näin pidät huolta tietoturvasta kotona ja työpaikalla*, jossa esiintymiä oli yhteensä 12, joista yhdeksän edusti uhkapuheen kehystä ja kolme yhteiskunnallisen ulottuvuuden kehystä. Nämä yhdeksän uhkapuheen kehyksen esiintymää muodostivat myös suurimman yksittäisen kehysten esiintymän yhdessä artikkelissa. Kaikkiaan yhteenlaskettujen kehysten esiintymien määrä oli vähäisin TTN-artikkelissa *Nasevia neuvoja tiliesi turvaamiseksi*, josta löytyi vain yksi ilmentymä, joka edusti uhkapuheen kehystä.

Kehysten esiintymismäärät liittyvät usein materiaalin luonteeseen ja lyhyyteen, mutta myös esimerkiksi siihen, että materiaalissa pyritään antamaan ohjeita tai neuvoja ilman tilanteen suurempaa taustoitusta. Taustoituksen puute voi johtaa siihen, että esimerkiksi tilanteen muodostamaan uhkaan ei vedota juurikaan, jolloin uhkapuhetta ei esiinny. Toisaalta jos materiaalin tavoitteena on vain neuvoa tai ohjeistaa, niin yhteiskunnallinen puhe ei välttämättä sovellu tähän yhteyteen, eikä sitä siksi myöskään ilmene. Haastavaksi tilanteen tulkinnan tekee se, että vaikka Kyberturvallisuuskeskuksen sivuilla on oma erityinen Ohjeet ja oppaat -osionsa, niin erilaisia ajankohtaisia ohjeita ja neuvoja jaetaan runsaasti myös TTN-artikkeleina. TTN-artikkelit ovat monesti Ohjeet ja oppaat -osion ohjeistuksia lyhyempiä, ja ne keskittyvät selkeästi yhden hyvin rajatun haavoittuvuuden tai hyökkäyksen kuvailuun, sekä erityisesti tältä haavoittuvuudelta tai hyökkäykseltä suojautumiseen. Kohdeyleisön näkökulmasta TTN-artikkelien joukosta voi olla joskus myös haastavaa löytää itseä kiinnostavat artikkelit, koska kohderyhmiä ei ole TTN-kategoriassa jaoteltu valmiiksi kuten Ohjeet ja oppaat -osiossa.

Kuten jo mainittiin, eniten uhkapuheen kehyksen esiintymiä löytyi Ohjeet ja oppaat -osion artikkelista *Näin pidät huolta tietoturvasta kotona ja työpaikalla*, josta löytyi yhdeksän kehyksen esiintymää. Uhkapuhetta ilmenee Ohjeissa ja oppaissa ylipäätään tasaisemmin kuin TTN-artikkeleissa, joihin lukeutuu neljä artikkelia, joissa uhkapuheen kehystä ei ilmene ollenkaan, kun taas Ohjeiden ja oppaiden kategoriassa uhkapuheen kehystä esiintyy jokaisessa artikkelissa. Tämä voi johtua siitä, että Ohjeet ja oppaat ovat luonteeltaan kohdeyleisöään tietynlaiseen käyttäytymiseen houkuttelevia, ja tätä houkuttelua voidaan tehdä esimerkiksi epätoivottua käyttäytymistä seuraaviin uhkiin vetoamalla, kuten suojelumotivaatioteoriassakin on ajatuksena. Uhkapuhetta koskevassa alaluvussa 4.2 esitellään aineistossa esiintyviä kehyksiä tarkempien esimerkkien ja sitaattien avulla.

Kuten todettu, TTN-aineistojen joukossa on peräti neljä artikkelia, joissa uhkapuheen kehystä ei esiinny ollenkaan. Näihin lukeutuu esimerkiksi Tietoturvan vuosi 2018 -katsauksen pääkirjoitus *Kyberturvallisuus kuuluu kaikille*, sekä tehtävänsä jättävän Kyberturvallisuuskeskuksen ylijohtajan jäähyväispuheenvuoro *Yhteiskuntamme haavoittuvuuksia ei korjata vain keskustelemalla*. Huomionarvoista on, että nämä molemmat ovat saman henkilön kirjoittamia, ja tyyliltään yleisluontoisia puheenvuoroja. Kaksi muuta artikkelia, joissa uhkapuhetta ei

esiintynyt ollenkaan, ovat puolestaan luonteeltaan selkeästi tiedotteita: #*tietoturvatorstai - Ota arjen tietoturva haltuun asiantuntijoidemme kanssa* sekä *Kyberturvallisuuden superkuukausi on täällä taas!* Se, ettei uhkapuhetta esiinny mainituissa artikkeleissa voi johtua monista seikoista. Tiedotteissa ja erityisesti yleisissä puheenvuoroissa on ehkä tietoisesti haluttu ottaa optimistisempi linja, ja kuvata tietoturvaa positiivisemmassa valossa. Tämä voi puolestaan johtua halusta lisätä toiveikkuutta tulevasta. Jos tietoturvasta puhuttaisiin aina vain uhkien kautta, se saattaisi lisätä koettua turvattomuuden tunnetta ja jopa toivottomuutta, erityisesti, jos ei samalla puhuttaisi ollenkaan siitä, mitä näille uhille voidaan tehdä. On mahdotonta sanoa tämän tutkimuksen puitteissa, onko uhkapuhetta vältelty näissä kyseisissä artikkeleissa tietoisesti, mutta joka tapauksessa ne toimivat todisteena siitä, että tietoturvasta voidaan puhua ja puhutaan ilman uhkanäkökulmaa.

Siinä missä mainituissa yleisluontoisemmissa puheenvuoroissa vältellään uhkapuhetta, niin yhteiskunnallista puhetta niissä esiintyy senkin edestä. Sama *Kyberturvallisuus kuuluu kaikille* -artikkeli sisälsi nimittäin, yhdessä artikkelin *Suomi aloittaa älylaitteiden turvallisuuden varmistamisen ensimmäisenä Euroopassa – uusi Tietoturvamerkki auttaa kuluttajia tekemään turvallisempia kodin älylaitehankintoja* kanssa, eniten yhteiskunnallisen ulottuvuuden kehyksen esiintymiä, kummassakin kahdeksan kappaletta. Huomioitavaa on, että nämä ovat molemmat juuri TTN-artikkeleja. TTN-artikkeleissa yhteiskunnallista puhetta ilmenee Ohjeita ja oppaita enemmän todennäköisesti siksi, koska TTN-artikkelien joukkoon lukeutuu luonteeltaan yleisempiä tekstejä, kuten Tietoturvan vuosi -katsausten esipuheita ja muita tietoturvasta yleisemmällä tasolla kertovia artikkeleja kuten tiedotteita. Koska Kyberturvallisuuskeskus on Suomen kansallinen tietoturvatoimija, erityisesti keskuksen johdon puheenvuorot voidaan tulkita myös yhteiskunnallisiksi kannanotoiksi, jolloin on luontevaa, että ne sisältävät yhteiskunnallisen ulottuvuuden kehystä. Ohjeet ja oppaat puolestaan sisältävät varsin aihespesifejä ohjeistuksia, joiden tarkoitus on nimensä mukaisesti tarjota nimenomaan ohjeita yleisemmän tiedottamisen sijaan. Ohjeissa ei aina ole mielekästä puhua tietoturvasta yhteiskunnallisesta näkökulmasta. Tämän takia vaikuttaa luonnolliselta, että yhteiskunnallista puhetta ilmenee enemmän juuri TTN-artikkelien joukossa.

Ohjeiden ja oppaiden kategoriassa yhteiskunnallisen puheen kehystä esiintyy puolestaan enimmillään neljästi kahdessa eri artikkelissa: *Turvallisuusopas poikkeusolojen jälkeiseen aikaan* ja *Salasanat haltuun – Kuka käyttää tiliäsi?* Yhteiskunnallisen ulottuvuuden kehystä esiintyy näin ollen vähemmän Ohjeissa ja oppaissa kuin TTN-artikkeleissa. Lisäksi huomionarvoista on, että Ohjeiden ja oppaiden kategorian kymmenestä aineistosta neljässä ei esiinny yhteiskunnallisen ulottuvuuden kehystä ollenkaan. Nämä havainnot tukevat ajatusta siitä, että yhteiskunnallinen puhe ilmenee enemmän yleisluontoisemmissa teksteissä ja tiedotteissa, jotka kertovat tietoturvasta yleisesti tai jotka käsittelevät ilmiötasoa yksityiskohtaisten ohjeistusten sijaan.

Määrällinen analyysi on jo paljastanut monia kiinnostavia seikkoja aineistosta. Seuraavaksi siirrytään tarkastelemaan aineistoa tarkemmin havainnollistavien sitaattien kera kehys kerrallaan. Ensin käsitellään uhkapuheen kehys,

jonka jälkeen vuorossa on yhteiskunnallisen ulottuvuuden kehyksen tarkastelu. Analyysissa viitattavat aineistot on koottu omaksi lähdeluettelokseen liitteeseen 1.

4.2 Uhkapuheen kehys

Uhkapuheen kehys juontuu, kuten aiemmin jo mainittiin, suojelumotivaatioteoriasta. Uhkapuheen kehykseen liittyy näin ollen kaikki se puhe, jolla voidaan pyrkiä vaikuttamaan siihen, miten kohdeyleisö arvioi uhkaa, tai miten he arvioivat selviytyvänsä uhasta. Kuten aiemmin alaluvussa 2.4 kerrottiin, suojelumotivaatioteorian mukaan ihmisten arvioon uhasta vaikuttaa kolme asiaa, jotka ovat epätoivottavasta käyttäytymisestä seuraavat hyödyt, uhan vakavuus ja alttius uhalle (Floyd ym. 2000, 410). Näiden ohella suojelumotivaatioteoria määrittelee kolme tekijää, jotka vaikuttavat siihen, miten ihminen arvioi selviytyvänsä uhasta. Nämä tekijät ovat usko vastatoimien tehoon, vastatoimien kustannukset sekä minäpystyvyys (Vance ym. 2012, 190).

Kuten jo määrällisessä analyysissa todettiin, uhkapuhetta ilmenee aineistossa 75 kertaa varsin tasaisesti läpi aineiston, mutta vähän enemmän Ohjeet ja oppaat -osiossa. Uhkapuhetta esiintyy esimerkiksi tilanteissa, joissa kuvaillaan erilaisia tietoturvauhkia tai kerrotaan erilaisista vaaroista tai uhista, jotka ihmistä tietoturvan saralla voivat kohdata:

> ”Huijausviestit vievät tietosi ja rahasi” (Traficom 2020b)

> ”Päivittämättömän laitteen käyttö on aina riskialtista. Samalla kutsut tietomurrot kylään.” (Traficom 2020b)

Kuten näistä sitaateista nähdään, uhkapuhe voi joskus olla varsin suorasukaista. Esimerkeissä, kuten aineistossa usein muutenkin, puhutellaan lukijaa suoraan sinä-muodossa. Sitaateissa tietoturvauhkia kuvataan varsin ehdottomiksi, huijausviestit varmasti vievät tietosi sekä rahasi ja päivittämättömien laitteiden käyttö johtaa tietomurtoihin. Näin luodaan kuvaa siitä, että jos annettuja neuvoja ei noudateta, niin kuvatut uhat realisoituvat ehdottomasti. Huijausviestit eivät kuitenkaan tosiasiassa itsessään vie tietoja tai rahoja, vaan uhri itse huijattuna antaa huijarille pääsyn niihin. Sitaateissa on siis tietyllä tavalla vähän liioiteltu mainittuja uhkia, minkä tarkoituksena lienee saada ihmiset ottamaan uhat vakavasti, ja tarttumaan ehdotettuihin vastatoimiin. Sitaatit voidaankin näin ollen liittää suojelumotivaatioteorian ajatukseen, että ihmisten uhkia koskevaan arviointiin liittyy myös arviointi siitä, kuinka vakava uhka on, ja kuinka altis sille hän on. Kuvaamalla uhat väistämättöminä ne saadaan vaikuttamaan vakavilta ja ihmiset alttiimmilta niille. Tämä voidaan puolestaan nähdä yrityksenä houkutella ihmisiä käyttäytymään toivotulla, Kyberturvallisuuskeskuksen ehdottamalla tavalla uhan välttämiseksi.

Aineistossa viitataan paljon erityisesti uhalle alttiuteen, mitä tulee ihmisten uhista tekemiin arvioihin. Alttius uhalle ilmenee esimerkiksi puhuttaessa uhkien yleisyydestä tai tekijöistä, jotka altistavat uhille, kuten edellisessä esimerkissä mainittu laitteiden päivittämättömyys. Toisaalta alttius uhille voi esiintymiä myös paljon yleisemmissä yhteyksissä:

> ”Jos käytät internetiä, voit olla verkkorikollisen kohde.” (Traficom 2020h)

> ”Huijaukset, tietomurrot ja tietovuodot koskevat meistä jokaista.” (Traficom 2021a)

Näissä esimerkeissä alttius uhalle vedetään varsin äärimmäiselle tasolle: kaikki Internetin käyttäjät voivat olla alttiita verkkorikollisuudelle. Ensimmäinen lainaus esiintyi kyseisen aineiston, joka lukeutuu Ohjeet ja oppaat -osioon, alkupäässä, jossa sen tarkoituksena voidaan tulkita olevan pohjustaa tulevia ohjeita. Näin ollen esimerkin tarkoituksena voi olla lisätä lukijan myötämielisyyttä tulevia ohjeita kohtaan vetoamalla siihen, kuinka lukijakaan ei ole näiltä uhilta turvassa.

Alttiudesta uhalle puhutaan usein myös vetoamalla uhan yleisyyteen:

> ”Moneen internetissä käytettyyn palveluun on kohdistunut suuria salasanavuotoja. Jopa miljoonia käyttäjätunnus-salasana-pareja on vuodettu yleisesti saataville.” (Traficom 2020g)

Tämä voidaan perustella niin, että jos sitaatin sanoin moneen palveluun on kohdistunut suuria vuotoja, joissa on vuodettu miljoonia käyttäjätunnuksia ja salasanoja, uhka on niin yleinen, että se voi osua kenen tahansa kohdalle. Mitä yleisempi jokin uhka on, tai mitä enemmän tietoja vuotaa tietovuodoissa, sitä todennäköisempää on, että ennemmin tai myöhemmin uhka realisoituu omallakin kohdalla. Näin ollen vetoamalla uhan yleisyyteen pyritään saamaan lukija uskomaan, että hän on itsekin altis uhalle, ja siksi hänen tulisi kiinnittää huomiota omaan tietoturvakäyttäytymiseen. Tähän liittyy myös toisessa artikkelissa huomioitu yleinen harhaluulo omasta koskemattomuudesta:

> ”Mitä menetettävää minulla muka on?” (Traficom 2020h)

> ”Kun henkilö tai organisaatio arvioi omaa riskiään joutua tietoturvapoikkeaman kohteeksi, oletetaan että on oltava hyökkääjää kiinnostava kohde, vaikka tyypillisesti kohteeksi päädytään sattumanvaraisesti.” (Traficom 2020c)

Jälkimmäinen sitaatti pyrkii kumoamaan usein kuullun perustelun sille, miksi omaan tietoturvaan ei koeta tarvetta panostaa: enhän minä ole hyökkääjää kiinnostava kohde. Muistuttamalla, että tietoturvapoikkeaman uhriksi joudutaan usein sattumanvaraisesti, yritetään murtaa tätä harhaluuloa. Jos hyökkäykset suunnataan sattumanvaraisesti, voi todennäköisyys uhriksi joutumiseen näyttäytyä yksilön näkökulmasta suuremmalta kuin siinä tapauksessa, jos ajatellaan uhriksi päädyttävän vain esimerkiksi statuksen myötä. Näin ollen sitaatin tarkoituksena voidaan tulkita olevan lisätä lukijan kokemusta omasta alttiudes-

taan uhalle, ja siten edistää ihmisen halua käyttäytyä toivotulla tavalla eli tietoturvallisemmin.

Uhkien yleisyyttä ja siten lukijan kokemusta uhalle alttiudesta luodaan myös kuvaamalla sitä, miten tietoturva vaikuttaa myös paikoissa ja yhteyksissä, joita ei tulisi heti ajatelleeksi:

> ”Kodissasi piilee älykkyyttä, ehkä enemmän kuin olet tullut ajatelleeksi.” (Traficom 2020m)

Tässä esimerkissä asiayhteytenä on älylaitteiden tietoturva, joka saattaa olla monelle lukijalle aikaisemmin tuntemattomampi tietoturvan osa-alue. Sitaatissa uhan yleisyyttä pyritään korostamaan muistuttamalla, että älylaitteidenkin tietoturvasta täytyy huolehtia. Yksityishenkilöille voi olla vieras ajatus, että myös esimerkiksi älyjääkaappi tai -televisio voisi sisältää tietoturvahaavoittuvuuksia. Älylaitteiden yleistyessä muistutus on todennäköisesti katsottu tarpeelliseksi, jotta myös yksityishenkilöt ymmärtäisivät näiden uhkien yleisyyden, ja ymmärtäisivät siten mukauttaa omaa käyttäytymistään sen mukaan.

Uhalle alttiuden ohella suojelumotivaatioteoria pitää uhkien arviointiprosessissa tärkeänä arviota uhan vakavuudesta. Uhan vakavuuteen viitataan aineistossa esimerkiksi tilanteissa, joissa kuvataan tietoturvauhkien realisoitumisesta mahdollisesti seuraavia haittoja:

> ”Rahan, henkilötietojen tai omien valokuvien menettäminen aiheuttaa paljon harmia, eikä kaikkia menetettyjä tietoja välttämättä saa takaisin.” (Traficom 2019f)

Tässä esimerkissä kuvataan ensinnäkin sitä, mitä asioita tietoturvaloukkaukset voivat vaarantaa: uhrin rahat, henkilötiedot ja valokuvat. Lisäksi esimerkissä painotetaan uhan vakavuutta toteamalla, ettei menetettyjä tietoja saa välttämättä koskaan takaisin. Viittaamalla mahdollisiin tietoturvaloukkauksen myötä menetettäviin asioihin pyritään lisäämään kohdeyleisön käsitystä siitä, mitä on vaakalaudalla, jos joutuu tietoturvaloukkauksen uhriksi. Tällaisella puheella voidaan vedota esimerkiksi ihmisiin, jotka eivät ymmärrä, mitä menetettävää heillä oikeastaan on. Jos ihminen ei ymmärrä tietoturvaloukkausten seurauksia, ei hän välttämättä näe syytä käyttäytyä tietoturvallisella tavalla. Näin vetoamalla eri asioihin, jotka ovat ihmisille tärkeitä, pyritään kannustamaan ihmisiä tietoturvallisempaan käyttäytymiseen, jotta uhka voitaisiin välttää. Mainitsemalla sekä rahan, henkilötiedot että valokuvat yritettäneen vedota mahdollisimman moneen eri yleisöön samanaikaisesti, sillä eri ihmiset arvottavat asioita eri tavalla. Vetoamalla kaikkiin kolmeen pyritään tavoittamaan ne, jotka pitävät jotakin näistä arvossa. Esimerkki saa vielä lisää tehoa lisäämällä perään, ettei menetettyjä tietoja saa välttämättä takaisin, mikä edistää mielikuvaa uhan vakavuudesta, ja kannustaa siten ihmisiä tietoturvallisempaan käyttäytymiseen ennen kuin on liian myöhäistä.

Siinä missä edellinen esimerkki keskittyi kuvaamaan sitä, mikä kaikkea voidaan menettää tietoturvaloukkauksen seurauksena, niin aineistossa on viittauksia myös siihen, mitä menetetyillä tiedoilla voidaan saavuttaa:

> ”Puhelinnumero, nimi ja osoite voivat saada rikolliset liikkeelle, jopa vieraiksi pankkitilillesi ja kotiisi asti.” (Traficom 2020e)

> ”Huijari voi kiristää ja uhkailla sinua esimerkiksi maineen ja omaisuuden menettämisellä. ” (Traficom 2021b)

Sitaateissa ollaan edellistä esimerkkiä konkreettisemmalla tasolla, kun kuvataan, miten vääriin käsiin päätyneet tiedot voivat auttaa rikollisia pääsemään käsiksi uhrin pankkitilin sisältöön tai jopa uhrin kotiin, tai johtaa maineen ja omaisuuden menettämiseen. Siinä missä edellisessä esimerkissä laskettiin sen varaan, että kohdeyleisö ymmärtää uhkan vakavuuden jo vaarantuvien tietojen perusteella, niin tässä esimerkissä selitetään vieläkin tarkemmin, miksi tällaisten tietojen päätyminen vääriin käsiin on epätoivottavaa. Myös näissä esimerkeissä viitataan moniin eri asioihin, maineeseen, omaisuuteen ja kotirauhaan, jolloin voidaan vedota erilaisiin kohderyhmiin, sillä eri ihmisten henkilökohtaiset arvomaailmat vaikuttavat siihen, mikä näistä heihin eniten vetoaa. Tietoturvaloukkausten mahdollisten seuraamuksien selittämisen tarkoituksena voidaan tulkita olevan saada kohdeyleisö ajattelemaan sitä, kuinka vakavasta uhasta tässä onkaan kyse, ja siten saada kohdeyleisö pohtimaan omaa tietoturvakäyttäytymistään.

Uhan vakavuuteen viitattiin aineistossa myös tietoturva-alan ja sen ilmiöiden nopeatempoisuuden ja nopean kehityksen kautta:

> ”Mennyt vuosi tullaan muistamaan myös uusien haavoittuvuuksien nopeasta hyödyntämisestä ---.” (Traficom 2020d)

> ”Löydettyjä tietoturva-aukkoja hyödynnetään yhä nopeammin.” (Traficom 2020c)

Näissä esimerkeissä uhan vakavuutta korostetaan puhumalla uusien tietoturvauhkien nopeasta hyödyntämisestä. Sitaateista saa kuvan, että tietoturvassa kehitys on nopeaa, ja tietoturvasta huolehtiakseen on pysyttävä kehityksessä mukana. Jos tietoturvan uusimmat käänteet eivät ole hallussa, eikä ihminen tunne uusia haavoittuvuuksia ja niiltä suojautumista, uhka voi realisoitua entistä nopeammin ja helpommin. Uusiin haavoittuvuuksiin oikeaoppisesti reagoiminen tarvittavan nopeasti voi olla tavalliselle yksityishenkilölle hyvin haastavaa, mikä tukee tulkintaa siitä, että tämä kehityskulku vaikuttaa nimenomaan uhan vakavuuden arviointiin. Toisaalta, jos ihminen ei tiedä, miten hänen tulisi käyttäytyä ja mitä hänen tulisi tietoturvasta milloinkin tietää, tällainen nopeasta kehityksestä ja sen vaaroista puhuminen voi herättää ihmisessä toivottomuutta tai turhautumisen tunnetta, jolloin ihmisen kannustaminen tietoturvakäyttäytymisen kehittämiseen voi muuttua haastavammaksi.

Myös todennäköisyyksiä käytettiin aineistossa hyväksi uhan vakavuuteen vedotessa:

> ”Haavoittuvilla järjestelmillä on aina suurempi riski joutua tietomurron kohteeksi.” (Traficom 2020g)

Sitaatin asiayhteys on laitteiden päivitysten ajantasaisuudesta huolehtiminen. Sitaatissa laitteiden tai järjestelmien päivittämättä jättäminen esitetään haavoittuvuutta lisäävänä tekijänä, ja haavoittuvuus puolestaan nähdään tietomurron uhriksi joutumista edesauttavana tekijänä. Näin ollen uhan vakavuus korostuu, jos järjestelmä on haavoittuva, eikä sitä ole päivitetty. Suurempi riski viittaa tässä yhteydessä siis suurempaan ja sen myötä myös vakavampaan uhkaan. Tämän sitaatin voidaankin tulkita pyrkivän vetoamaan varsin yksityiskohtaisen tietoturvakäyttäytymisen, eli päivittämisen, puolesta.

Suojelumotivaatioteorian mukaan uhan vakavuuden ja uhalle alttiuden lisäksi ihmisten tekemiin uhkien arviointiin vaikuttaa myös epätoivottua käyttäytymistä seuraavat hyödyt ja palkkiot. Näihin viitattiin aineistossa muita kahta jonkin verran vähemmän. Epätoivottua käyttäytymistä seuraaviin hyötyihin viitattiin kuitenkin esimerkiksi seuraavasti:

> ”Äiti: Siis kannattaa päivittää se, ettei kukaan pääse häkkään tuota.
> Lapsi: Mä en halua mitään häkkäystä, mä haluisin vain pelata.” (Traficom 2020o)

Vaikka lapsi ei tässä suoraan sanokkaan, ettei halua päivittää laitettaan, sitaatti voidaan tulkita niin, että lapsi haluaisi vain pelata, ilman että tarvitsisi välillä keskeyttää toiminta tietoturvatoimenpiteitä varten. Pelaaminen on tässä tapauksessa palkinto tai hyöty, joka epätoivottua käyttäytymistä, eli laitteen tietoturvapäivitysten ajamatta jättämistä, seuraisi. Toisaalta sitaatin keskustelussa yritetään saada tämä epätoivottu käyttäytyminen näyttäytymään epämieluisalta palkinnoista huolimatta kuvaamalla päivittämättä jättäminen hakkeroinnille altistavana tekijänä. Tavoitteena voidaan ajatella olevan saada kohdeyleisö valitsemaan tietoturvallinen käyttäytyminen palkintojen sijaan, tai muuten hakkerit voivat iskeä.

Uhkien arvioinnin lisäksi suojelumotivaatioteoria pyrkii selittämään, miten ihminen arvioi mahdollisuuksiaan selviytyä uhasta. Teorian mukaan yksi tekijä, joka tähän vaikuttaa, on usko vastatoimien tehoon uhkaa vastaan. Aineistossa tämä ilmenee esimerkiksi viittauksilla siitä, miten annettuja ohjeita noudattamalla voi välttää mainittuja tietoturvauhkia:

> ”[L]ähes kaikki tilien kaappausyritykset voidaan estää monivaiheista tunnistautumista käyttämällä.” (Traficom 2021d)

> ”Kun on varautunut tulevaan mahdollisimman hyvin, toimintakyky säilyy tilanteessa kuin tilanteessa.” (Traficom 2020c)

> ”Kun kodin verkkoon liitettyjen laitteiden kuten älytelevisioiden ja -puhelimien ja lelujen tietoturva on kunnossa, vältytään esimerkiksi tietojen väärinkäytöltä, laitteiden haltuunotoilta tai tietovuodoilta.” (Traficom 2019h)

Näistä esimerkeistä ensimmäinen on konkreettisin ja antaa selkeän kehotuksen tietynlaiseen käyttäytymiseen, monivaiheisen tunnistautumisen käyttämiseen. Toiset kaksi puolestaan viittaavat epämääräisemmin hyvään varautumiseen ja tietoturvan kunnossapitämiseen keinona uhkia ja niiden realisoitumisen aiheut-

tamia haittoja vastaan. Haasteena näissä jälkimmäisissä on juurikin niiden abstraktimpi taso, jolloin lukija ei välttämättä tiedä, mitä hänen olisi tarkalleen tehtävä uhkia torjuakseen. Lukijalle vakuutetaan, että vastatoimet toimivat, mutta jos hän ei tiedä, miten niitä käytännössä toteuttaa, voi toivottuun käyttäytymiseen ryhtyminen olla epätodennäköisempää. Toisaalta on hyvä huomioida, että viimeisin sitaatti on artikkelista, jossa esiteltiin uuden Tietoturvamerkin käyttöönottoa, jolloin viimeinen sitaatti voidaan tulkita niin, että ihmisiä kehotetaan ottamaan ostokäyttäytymisessään huomioon tuotteet, joille tällainen merkki on myönnetty, sillä se itsessään on todiste tietoturvasta. Tietoturvan alalla vastatoimien tehoon vetoaminen voi olla haastavaa, koska harva tietoturvauhilta suojaava menetelmä tarjoaa täydellistä turvaa, jolloin olisi väärin sellaista luvatakaan.

Vastatoimien tehon lisäksi ihmisten uhista selviytymisen arviointiin liittyvät myös vastatoimien kustannukset. Vastatoimien kustannuksiin ei juurikaan viitattu aineistossa. Tämä voi olla selitettävissä sillä, että monesti aineistossa kehotetaan kohdeyleisöä tietynlaiseen tietoturvakäyttäytymiseen, jolloin vastatoimien kustannuksista puhuminen voisi näyttäytyä epäkannustavana. Toisaalta Kyberturvallisuuskeskus ei kansallisena ja puolueettomana valtion virastona ota kantaa esimerkiksi tietoturvaloukkauksia vastaan suunnattujen vastatoimien aiheuttamiin taloudellisiin kustannuksiin, eikä erityisesti kehota kohdeyleisöä ostamaan jotakin tiettyä tietoturvatuotetta tai -palvelua. Vastatoimien kustannuksia voidaan myös ajatella siitä näkökulmasta, että mistä ihminen joutuu luopumaan mukauttaessaan käyttäytymistään annettujen ohjeiden mukaan. Tähänkään ei kuitenkaan suorasanaisesti aineistossa juurikaan viitata. Voidaan toisaalta pohtia, että voitaisiinko esimerkiksi hyvien salasanojen laatimiseen ja käyttöön kannustavat oppaat, kuten *Pidempi parempi – Näin teet hyvän salasanan* sekä *Salasanat haltuun – Kuka käyttää tiliäsi?* mieltää vastatoimien kustannuksia sivuaviksi aineistoiksi. Näissä oppaissa ohjeistetaan salasanaturvallisuuteen esimerkiksi mainitsemalla, että salasanojen tulisi olla pitkiä ja joka palvelussa ainutlaatuisia. Ohjeistus voi ehkä näyttäytyä kohdeyleisölle eräänlaisena kustannuksena, esimerkiksi aika- tai resurssikustannuksena, verrattuna siihen, että ihminen käyttäisi palveluihin kierrätettyjä, lyhyitä ja helposti muistettavia salasanoja. Hyvien salasanojen laatiminen vie ihmiseltä aikaa ja se vaatii pohtimista ja paneutumista, erityisesti jos ihminen aikoo noudattaa kehotusta laatia jokaiseen palveluun oman, uniikin salasanansa. Aineistossa ei kuitenkaan suoraan tuoda esiin tätä vastakkainasettelua.

Sen sijaan minäpystyvyyteen vedotaan aineistossa monin paikoin. Minäpystyvyys on kolmas suojelumotivaatioteorian nimeämä tekijä, joka vaikuttaa ihmisten arvioon uhasta selviytymisestä, ja sillä tarkoitetaan ihmisen arviota omasta kyvystään suorittaa uhalta suojautumisen edellyttämät toimenpiteet. Minäpystyvyyteen viitataan aineistossa esimerkiksi tilanteissa, jossa pyritään vakuuttamaan kohdeyleisö siitä, että toivottu tietoturvakäyttäytyminen on heidän tehtävissään:

> ”Esimerkiksi salasanan vaihtaminen ja päivitysten lataaminen kodin älylaitteisiin onnistuu myös sinulta.” (Traficom 2020m)

Tässä esimerkissä tietoturvallisempaan käyttäytymiseen kannustetaan luomalla kuvaa siitä, että tietoturvaa edistävät toimet ovat jokaisen tehtävissä. Tarkoituksena voi olla tavoittaa ne, jotka kokevat tietoturvaa parantavat toimenpiteet liian monimutkaisina ja vaikeina, jotta niistä voisi omin avuin selviytyä. Tällaiset kokemukset toivotun tietoturvakäyttäytymisen liiallisesta vaikeudesta voivat puolestaan olla ihmistä passivoivia. Näin ollen ajatuksena tällaisessa kannustavassa puheessa voikin olla juuri kohdeyleisön aktivoiminen luomalla heihin uskoa omiin kykyihinsä.

Kotiturvalistit-videosarjan Salasana-videossa aikuinen tytär auttaa äitiään salasanan vaihdossa ja monivaiheisen tunnistautumisen käyttöönotossa:

> ”Tytär: Pitäisikö siihen kerralla laittaa tommonen monivaiheinen tunnistautuminen?
> Eija-äiti: No, mikäs se on?
> ---
> Mies: Monimutkainen…
> T: Ei kun monivaiheinen. Voila!
> E: Nyt se tuli jo.
> T: Niin tuli
> E: No eihän tämä nyt ollut niin hankalaa.
> Kertoja: Eipä. Monivaiheinen tunnistautuminen ei todellakaan ole hankalaa.” (Traficom 2020n)

Edellä kuvattu sanailu pyrkii vahvistamaan mielikuvaa tietoturvaa edistävien toimien helppoudesta, ja siten vaikuttamaan minäpystyvyyden kokemukseen positiivisesti. Tällä esimerkillä yritettänee vedota erityisesti vanhempien ikäluokkien minäpystyvyyden tunteeseen, koska videossa monivaiheista tunnistautumista käyttöönottava Erja-äiti on kuvattu jo varttuneemmaksi hahmoksi. Näin voidaan pyrkiä luomaan kohdeyleisön kannalta samaistuttava esimerkki, jonka positiivisesta kokemuksesta voi rohkaistua ja ottaa mallia. Kun joku omasta näkökulmasta samaistuttava henkilö sanoo, että eihän se nyt niin hankalaa ollutkaan, niin se voi vahvistaa käsitystä omasta minäpystyvyydestä ja luoda uskoa, että kyllä minäkin pystyn, jos hänkin pystyi.

Minäpystyvyyteen pyritään vetoamaan myös epäsuoremmin sanomalla, että uhat ovat ehkäistävissä:

> ”Suurin osa huijareista ja huijauksista ovat tunnistettavissa ja torjuttavissa.” (Traficom 2019d)

Tässä esimerkissä ei edellisten tapaan vedota suoraan joidenkin tiettyjen tietoturvaa edistävien toimien helppouteen, vaan ennemminkin yleisellä tasolla todetaan, että kyseisille tietoturvauhille voidaan tehdä jotain. Näin ollen minäpystyvyyden kokemusta voidaan yrittää parantaa tässä laajemmin. Siinä missä aikaisemmissa esimerkeissä puhuteltiin lukijaa suoraan, tai vedottiin toimien helppouteen, tässä sitaatissa korostuu toivo siitä, että uhkien edessä ei kannata täysin lannistua, vaan tehdä niitä toimenpiteitä, joilla uhka on torjuttavissa. Minäpystyvyyden kokemus voi vahvistua, jos kohdeyleisö ajattelee, että uhka ei ole täysin väistämätön, vaan sen torjumiseksi voi oikeasti tehdä jotain. Tilateen

esittäminen toiveikkaana saattaa edistää kohdeyleisön motivoitumista tietoturvallisempaan toimintaan.

Edelliset esimerkit kuvaavat minäpystyvyyteen vetoamista positiivisessa valossa. Aineistosta ilmeni kuitenkin myös esimerkkejä, joilla on potentiaalia herättää kohdeyleisössä jopa minäpystyyttä kyseenalaistavia tai heikentäviä kokemuksia. Ensinnäkin kohdeyleisö laitettiin pohtimaan omaa minäpystyvyyttään:

> ”Kännykkäsi, äly-tv:si ja tietokoneesi sisältävät varmasti arvokasta tietoa sinusta. Osaatko huolehtia niiden turvallisuudesta ja päivityksistä?” (Traficom 2020b)

Tässä kysymykseksi muotoillussa esimerkissä tavoitteena lienee saada kohdeyleisö punnitsemaan omaa osaamistaan ja omia kykyjään toimia tietoturvallisella tavalla. Sitaatissa ei kuitenkaan erityisemmin rohkaista kohdeyleisöä tai luoda uskoa omiin kykyihin toisin kuin aikaisemmissa esimerkeissä. Muotoilunsa takia tämä esimerkki tuskin toimii yhtä tehokkaasti minäpystyvyyden kokemusta edistävänä tekijänä, erityisesti jos lukija päätyy vastaamaan kysymykseen kielteisesti. Esimerkissä ei anneta välittömästi ohjeita tai neuvoja siihen, miten lukijan tulisi toimia, jos ei koe omia tietojaan ja taitojaan riittäviksi, mikä voi johtaa passivoitumiseen.

Vielä edellistä esimerkkiäkin negatiivisemmin minäpystyvyyteen voidaan tulkita vaikutettavan puheella esimerkiksi huijaussivustojen tunnistamisen haastavuudesta:

> ”Monimutkaisissa malleissa aidon sivun sisältö saatetaan kopioida reaaliajassa alkuperäiseltä sivustolta kalastelusivustolle, jolloin erottaminen ulkoasun perusteella on mahdotonta.” (Traficom 2020f)

> ”Väärennetyn verkkosivun osoite voi olla lähes sama kuin aidon sivuston ---. Väärennetyn sivun sisältökin näyttää melkein aidolta ---.” (Traficom 2021b)

Esimerkeissä luodaan kuvaa huijauksien tunnistamisen vaikeudesta, jopa mahdottomuudesta. Tällainen puhe tuskin edistää kokemusta minäpystyvyydestä, koska miten ihminen voisi kokea pystyvänsä tunnistamaan huijaukset ja olemaan lankeamatta niihin, jos se kuvataan hyvin vaikeaksi. Tosiasioita ei tietenkään sovi vääristellä minäpystyvyyden kokemuksen kohentamiseksi, mutta näissä tilanteissa olisi tärkeää, että kohdeyleisölle annettaisiin hyvät ohjeet uhkaa vastaan toimimiselle. Onkin tässä yhteydessä hyvä huomata, että molemmat esimerkkilauseet löytyivät asiayhteydestä, jossa sitaattien jälkeen kohdeyleisölle annettiin ohjeita uhan välttämiseen. Joka tapauksessa tämän kaltaiset puheet saattavat vaikuttaa minäpystyvyyden kokemukseen kielteisesti, ja siten heikentää kohdeyleisön tunnetta siitä, että heiltä löytyy toivotun tietoturvakäyttäytymisen edellyttämät tiedot ja taidot.

Tietyllä tavalla minäpystyvyyteen vaikuttamisena voidaan ymmärtää myös kaikki aineistossa annetut ohjeet ja käytännön neuvot. Tämä laajempi näkökulma on tulkittavissa niin, että nämä ohjeet pyrkisivät edistämään ihmisten tietoturvataitoja ja siten kokemusta siitä, että ihminen pystyy toteuttamaan tar-

vittavia toimenpiteitä ja siten toivottavaa tietoturvakäyttäytymistä. Kaiken kaikkiaan minäpystyvyyteen viitataan aineistossa enemmän kuin vastatoimien tehoon ja vastatoimien kustannuksiin, vaikka kaikkia viittauksia ei voidakaan täysin pitää minäpystyvyyttä edistävinä.

Kaikkiaan aineistossa esiintyi paljon uhkapuhetta, joka oli yhdistettävissä johonkin suojelumotivaatioteorian osa-alueeseen. Uhkapuheessa selkeästi korostui ihmisten uhka-arviointiin liittyvät vetoomukset, erityisesti uhan vakavuuteen ja uhalle alttiuteen vetoava puhe. Sen sijaan epätoivottua käyttäytymistä seuraavat hyödyt ja palkinnot jäivät kahden edellä mainitun tekijän varjoon. Ihmisten uhka-arvioihin vetoamista jonkin verran vähemmän aineistossa käsiteltiin ihmisten arvioita siitä, miten hän selviytyisi uhasta. Tällä saralla eniten huomiota kiinnitettiin minäpystyvyyteen, samalla kun vastatoimien tehoon ja vastatoimien kustannuksiin vetoaminen jäi selvästi vähemmälle.

Näistä havainnoista voidaan päätellä, että Kyberturvallisuuskeskuksen yksityishenkilöille suunnatuissa viestintämateriaaleissa esiintyvä uhkapuhe keskittyy uhkien arvioinnin ympärille. Ihmisten omaa selviytymistä koskeviin arvioihin ei pyritä vetoamaan yhtä paljon kuin itse uhkien arviointiin. Koska uhkapuheessa korostuivat erityisesti uhan vakavuus sekä alttius uhalle, voidaan pohtia, herättääkö aineisto kohdeyleisössä liikaa pelon tunnetta. Bada ym. (2019) muistuttavat, kuten teoreettisen viitekehyksen luvussa jo todettiin, että tietoturvakampanjoiden haasteiksi muodostuu usein niiden liiallinen pelon lietsonta. Uhkapuheen kehyksen perusteella tämä huoli vaikuttaa aiheelliselta. Toisaalta tietoturvasta voi olla haastavaa puhua, erityisesti suojelumotivaation eri osa-alueisiin vedoten, herättämättä kohdeyleisössä yhtään pelkoa. Suojelumotivaatioteoriassa pelon ajatellaankin toimivan tiettyyn pisteeseen asti toimintaan motivoivana tekijänä. Tässä yhteydessä olisi hyvä löytää jonkinlainen kultainen keskitie, jossa pelon lietsonta ei pääse äitymään liialliseksi. Uhkien kuvailu on kuitenkin tärkeää, jotta kohdeyleisö pystyy saavuttamaan paremman ymmärryksen tietoturvauhista, mutta uhkien kuvailun vastapainoksi tietoturvaviestinnän olisi hyvä tuoda entistä enemmän esiin myös suojelumotivaation toista osa-aluetta, ihmisten arviota uhista selviytymisestä. Erityisesti vastatoimien tehosta ja vastatoimien kustannuksista, mutta myös minäpystyvyydestä olisi hyvä puhua entistä enemmän, jotta uhkien ymmärtämisen ohella kohdeyleisö oppisi paremmin toimimaan tietoturvauhkia vastaan, sekä uskomaan omiin tietoihinsa ja taitoihinsa.

4.3 Yhteiskunnallisen ulottuvuuden kehys

Toinen analyysissa tarkasteltavista kehyksistä on yhteiskunnallisen ulottuvuuden kehys. Kuten jo aiemmin todettiin, kehys voidaan jakaa kahteen eri osa-alueeseen: vaihtokauppapuheeseen sekä muutospuheeseen. Vaihtokauppapuhe viittaa viesteihin, joilla tarjotaan sosiaalisen markkinoinnin ytimessä olevaa vaihtokauppaa tai vastavuoroisuutta, kun taas muutospuhe tarkoittaa puhetta muutoksesta tai tietoturvan yhteiskunnallisesta merkityksestä. Yhteiskunnalli-

sen ulottuvuuden kehys pohjautuu näin ollen sosiaalisen markkinoinnin teoriaan, jonka keskiössä on vastavuoroisuus tai vaihtokauppa, ja jonka tarkoituksena on tavoitella markkinoinnin keinoin laajempaa yhteiskunnallista muutosta.

Muutospuhetta esiintyi aineistossa esimerkiksi tilanteissa, joissa kuvaillaan kehityskulkuja ja uusia ilmiöitä:

> ”Älykotien yleistyessä Suomessa verkkoon liitetään jatkuvasti enemmän laitteita, joiden välittämää tietoa käytetään erilaisissa palveluissa. Koska laitteet myös keräävät jatkuvasti tietoa käyttäjistään, tulee niiden tietoturvallisuuteen kiinnittää yhä tarkemmin huomiota.” (Traficom 2019h)

> ”Henkilö 1: Eikö nykypäivänä hakkerit pysty tunkeutumaan mihin tahansa älylaitteisiin?” (Traficom 2020m)

Esimerkissä muutoksesta puhutaan kuvaamalla hakkereiden kasvanutta hyökkäyskyvykkyyttä sekä älylaitteiden lisääntymistä kodeissa, mikä on johtanut siihen, että niiden tietoturvastakin tulisi pitää yhä paremmin huolta. Tällaisella puheella viitataan tietoturvan kasvavaan merkitykseen nyky-yhteiskunnassa, minkä myötä tietoturvaa ei voi enää ohittaa edes kodeissa. Tavoitteena voi olla luoda kuvaa tietoturvasta yhä merkittävämpänä, yksityishenkilöiden tavalliseen elämään linkittyvänä asiana, jolla kohdeyleisölle voidaan perustella heidän käyttäytymisessään tarvittava muutos tietoturvallisempaan suuntaan. Pyrkimys käyttäytymisen ja asenteiden muuttamiseen voidaan näin ollen nähdä keinona tavoitella laajempaa yhteiskunnallista muutosta.

Muutoksesta puhutaan aineistossa myös viittaamalla laajemmin siihen, että ajat ovat muuttuneet:

> ”--- koronakevät on jättänyt jälkensä myös nettiarkeemme. Uusi aika vaatii uudistettuja ajattelu- ja toimintatapoja.” (Traficom 2020i)

> ”Mennyt vuosi tullaan muistamaan myös uusien haavoittuvuuksien nopeasta hyödyntämisestä, --- ja käänteestä, jolloin huijauksista ja tietojenkalastelusta tuli arkeamme – uusi normaali.” (Traficom 2020d)

Uusi aika ja uusi normaali ovat käsitteitä, joilla luodaan kuvaa muutoksesta, joka vaatii kohdeyleisöltä toimenpiteitä. Kuvaamalla digitaalisessa ympäristössä tai sen tuomissa uhissa tapahtunutta muutosta voidaan perustella lukijalle, että tarve käyttäytymisen uudelleenarvioinnille sekä mukauttamiselle on todellinen. Erityisesti ensimmäisen sitaatin sanavalinnat kuvaavat muutoksen tarpeen välttämättömyyttä: uusi aika *vaatii* uudistettuja toimintatapoja. Käyttäytymisen muuttaminen esitetään välttämättömänä edellytyksenä uudessa ajassa selviämiselle, ja näin pyritään vaikuttamaan kohdeyleisön asenteisiin.

Tietoturvan merkityksen kasvusta yhteiskunnassa puhutaan aineistossa myös edellisiä esimerkkejä laajemmasta näkökulmasta, koko yhteiskunnan mittakaavassa:

> ”Kyberturvallisuus on yhteiskunnan turvallisuuden ja digitalisoitumisen perusedellytys.” (Traficom 2020a)

> ”Yhteiskunta tarvitsee tietoturvallisia arjen tekoja” (Traficom 2020d)

> ”Kyberturvallisuus kuuluu kaikille” (Traficom 2019c)

Nämä esimerkit kuvaavat sitä, miten tietoturva halutaan kuvata yhteiskunnallisesti yhä merkittävämmäksi tekijäksi. Yhteiskunnallisen merkityksen kasvun avulla voidaan perustella sitä, miksi laajempaa käyttäytymisen muutosta tarvitaan. Erityisesti kahdessa jälkimmäisessä sitaatissa vaikuttaa siltä, kuin puhe kohdistettaisi erityisesti tavallisille kansalaisille. Puheet arjen tietoturvateoista sekä siitä, miten kyberturvallisuus kuuluu kaikille, voidaan tulkita laajempaan yhteiskunnalliseen muutokseen rohkaiseviksi, koska niissä korostetaan tietoturvan arkipäiväisyyttä ja kuvataan tietoturva tärkeänä osana jokaisen elämää. Taustalla saattaa piillä ajatus, että yksityishenkilöt halutaan sitouttaa yhä tiiviimmin mukaan tietoturvalliseen toimintaan, ja luoda heille kokemusta siitä, että tietoturva koskettaa myös heitä. Kokemus tietoturvan henkilökohtaisesta merkityksestä saattaa edesauttaa asennemuutosta sekä käyttäytymisen muutosta tietoturvallisempaan suuntaan, mikä puolestaan johtaisi laajempaan yhteiskunnalliseen muutokseen kohti kaikille tietoturvallisempaa yhteiskuntaa.

Varsinaisesta muutoksesta puhumisen lisäksi muutospuheeseen voidaan lukea myös osaamista ja sen edistämistä koskeva puhe.

> ”Omasta tietoturvasta huolehtiminen on tärkeä taito digitaalisessa maailmassa.” (Traficom 2019f)

> ”Tietoturvasta huolehtiminen on digitaalisen elämäntapamme kansalaistaito.” (Traficom 2019g)

> ”Inhimillisen tietoturvan merkitystä ei saa unohtaa eikä aliarvioida. Kyberturvallisuudesta ei voi tulla arjen kansalaistaitoa, jos emme viesti siitä inhimillisesti ja ymmärrettävästi.” (Traficom 2019c)

Edellä olevissa esimerkeissä tietoturvataitoja kuvataan pariinkin otteeseen kansalaistaidoksi. Tietoturvasta halutaan luoda kuvaa yleishyödyllisenä osaamisena, johon jokaisella on paitsi oikeus myös velvollisuus. Voidaan tulkita, että esittämällä tietoturvasta huolehtimisen arjen kansalaistaitona tavoitteena on vaikuttaa kohdeyleisön asenteisiin tietoturvan tärkeyttä kohtaan. Kuten jo uhkapuheen kehyksen tarkastelussa todettiin, yksityishenkilöt saattavat joskus tuudittautua valheelliseen turvallisuudentunteeseen ja ajatella, että eihän heillä ole mitään menetettävää, tai ettei kukaan hakkeri kiinnostuisi juuri heistä, koska eiväthän he ole yhtään kiinnostavia kohteita. Luomalla kuvaa tietoturvasta niin tärkeänä, että sitä voidaan kutsua jo kansalaistaidoksi, voidaan yrittää puuttua liian huolettomaan suhtautumiseen tietoturvaa kohtaan. Näin ollen tämä voidaan tulkita pyrkimyksenä vaikuttaa asenteisiin ja edistää siten laajempaa yhteiskunnallista muutosta.

Tietoturvataitojen ja niiden kehittämisen tärkeydestä kertoo myös se, että ne olivat Euroopan kyberturvallisuuskuukauden keskiössä vuonna 2020. Aineistossa tähän viitataan positiivisesti ja kannustavasti:

> ”Kampanja on tarkoitettu meille kaikille. Laitetaan yhdessä kyberturvallisuuden perustaidot kuntoon!” (Traficom 2020l)

Esimerkissä tietoturvaosaamisen kehittämiseen kannustetaan puhumalla siitä, miten tietoturvan edistäminen on kaikkien yhteinen asia. Myös sitaatin kieli on kannustavaa, kun puhutaan me-muodossa ja yhdessä tekemisestä. Tietoturvan perustaidot kuvataan esimerkissä asiaksi, joka on syytä olla kunnossa kaikilla ihmisillä. Tässäkin näin ollen pyritään vakuuttamaan kohdeyleisö siitä, että tietoturva vaatii heidän toimenpiteitään.

Yksityishenkilöiden osaamista ja sen merkitystä yhteiskunnan tietoturvan kannalta sivutaan myös Tietoturvamerkistä puhuttaessa:

> ”Traficom haluaa Tietoturvamerkillä lisätä kuluttajien tietoisuutta tietoturvasta ja laitteiden tietoturvallista käyttöä.” (Traficom 2019h)

Tietoturvamerkin tarkoituksena on helpottaa tietoturvallisten tuotteiden tunnistamista ja valintaa. Sitaatin mukaan Tietoturvamerkillä tahdotaan vaikuttaa kohdeyleisön tietoturvatietoisuuteen ja helpottaa tietoturvallista käyttäytymistä erityisesti laitevalintojen osalta. Myös Tietoturvamerkin käyttöönotto itsessään voidaan tietyssä mielessä ymmärtää laajemman yhteiskunnallisen muutoksen ajamiseksi. Tietoturvasta tehdään yhä tarkemmin tarkasteltu ominaisuus, jonka toteutumisen seuraaminen pyritään tekemään tavalliselle kansalaisellekin mahdollisimman helpoksi.

Tietoturvamerkkiä koskeva sitaatti onkin myös erinomainen esimerkki seuraavasta yhteiskunnallisen ulottuvuuden kehyksen osa-alueesta, eli vaihtokauppapuheesta. Sosiaalisen markkinoinnin teorian mukaan markkinoinnin hyödyntäminen ihmisten käyttäytymiseen vaikuttamiseen on mahdollista vain, jos siihen sisältyy jonkinlainen vaihtokauppa tai vastavuoroisuus (Rothschild 1999, 24). Tämä ajatus perustuu siihen, ettei nykytilanteeseen tyytyväinen ihminen ole valmis muuttamaan toimintaansa, ellei koe saavansa jotain vastineeksi (Rothschild 1999, 26). Mainitussa tilanteessa toivottu käyttäytyminen, jota yritetään ajaa, on tietoturvallisempien laitteiden ostaminen. Tämä on pyritty tekemään tavallisille ihmisille mahdollisimman helpoksi Tietoturvamerkin avulla, kuten sitaatistakin käy ilmi. Tietoturvamerkki toimii ikään kuin lupauksena tai takuuna siitä, että laitteen tietoturvaan on kiinnitetty huomiota, jolloin ihminen voi toteuttaa toivottua tietoturvakäyttäytymistä suosimalla tällaisia laitteita. Vaihtokauppa siis on, että ihmistä suostutellaan muuttamaan käyttäytymistään tietoturvallisempaan suuntaan tarjoamalla vastavuoroisesti keinoja tietoturvallisuuden arviointiin ja tekemällä näin siitä helpompaa. Ostamalla Tietoturvamerkin omaavan laitteen ihminen saa vastineeksi todistetusti tietoturvallisemman laitteen ja siten parantaa niin omaa kuin yhteiskunnallistakin tietoturvaa.

Vaihtokauppapuhetta esiintyy erityisesti aineistojen alussa tilanteissa, joissa pyritään innostamaan kohdeyleisöä lukemaan kyseinen artikkeli tai ohjeistus:

> ”Päivitetyillä ohjeillamme pidät huijarin kurissa – erossa rahoistasi ja kullanarvoisista tiedoistasi.” (Traficom 2019d)

> ”Jos tunnistat verkkohuijaukset, päivität älylaitteesi ja käytät hyviä salasanoja, tärkeät tietosi pysyvät turvassa.” (Traficom 2020b)

Esimerkeissä vaihtokauppa muodostuu, kun vastineeksi käyttäytymisen muuttamisesta luvataan tietoturvallisuutta. Ensimmäisessä sitaatissa luvataan hyvin konkreettisesti, että toimimalla tietyllä tavalla lukija voi välttää rahojensa ja tietojensa vaarantumisen, eli saa siten käyttäytymisestään vastineeksi turvaa rahojen ja tietojen menettämistä vastaan. Toisessa sitaatissa puhutaan vähän epätarkemmin tärkeistä tiedoista, mutta joka tapauksessa luvataan niiden pysyvän turvassa, jos noudattaa toivottua tietoturvakäyttäytymistä.

On kuitenkin hyvä pitää mielessä, että Rothschildin (1999, 26–27) mukaan sosiaalisen markkinoinnin haasteena on luvattujen palkintojen summittaisuus, ja palkinnot ovatkin usein saavutettavissa vasta joskus tulevaisuudessa, jolloin vaihtokauppaan liittyy kohdeyleisön puolelta epävarmuutta. Turvallisuus saattaa myös näyttäytyä sellaisenaan liian epämääräiseltä palkinnolta, eikä vaihtokauppa siten välttämättä onnistu vaikuttamaan tarpeeksi houkuttelevalta. Toisaalta esimerkiksi omaisuuden, erityisesti rahallisen sellaisen, säilyttäminen saattaa olla tekijä, joka onnistuu vaikuttamaan tarpeeksi houkuttelevalta, jotta vaihtokauppa näyttäytyisi kannattavana kohdeyleisön näkökulmasta. Näin ollen edelliset esimerkit vaikuttavat ainakin pyrkivän välttämään tätä liiallista epämääräisyyden tasoa, josta Rothschild varoitti.

Lukijoille annetaan myös edellisiä esimerkkejä konkreettisempia neuvoja, jotka ohjeistavat hyvinkin yksityiskohtaisesti, miten olisi hyvä toimia tietyt tietoturvauhat välttääkseen:

> ”Salasanoja voi muodostaa ja tallentaa salasanaohjelmiin. Näin yksittäisiä salasanoja ei tarvitse muistaa ulkoa, kunhan muistaa apuohjelman salasanan.” (Traficom 2021d)

Tässä esimerkissä kehotetaan salasananhallintaohjelman käyttöön vetoamalla sen tuomiin etuihin, kuten mahdollisuuteen luoda salasanoja ohjelman avulla ja tallentaa niitä ohjelmaan. Esimerkissä vaihtokauppana tarjotaan elämää, jossa kaikkia salasanoja ei tarvitse enää muistaa itse, vaan pelkästään salasananhallintaohjelman salasanan muistaminen riittää. Vaihtokaupan houkuttelevuus perustuu tässä sitaatissa ajatukseen, että mukauttamalla käyttäytymistään tietoturvalliseksi, eli ottamalla käyttöön salasananhallintaohjelman, lukija pääsee nauttimaan helpommasta digitaalisesta elämästä, kun hänen ei enää tarvitse itse keksiä eikä muistaa salasanojaan.

Yhteiskunnallisen ulottuvuuden kehyksen voidaan ajatella esiintyvän aineistossa myös mainittuja esimerkkejä laajempana kokonaisuutena tilanteissa, joissa lukijalle pyritään antamaan neuvoja ja opettamaan keinoja, joilla erilaisia tietoturvauhkia vastaan voisi puolustautua. MOA-mallia esitellessään Rothschild (1999, 31–32) huomautti, että ihmisen tulee omata toivotun käyttäytymisen toteuttamiseksi tarvittavat tiedot ja taidot, jotta häneltä voidaan odottaa

käyttäytymisen muuttamista. Tämä ajatus linkittyy myös suojelumotivaatioteorian minäpystyvyyden ajatukseen, jossa ihminen arvioi mahdollisuuksiaan selviytyä uhista omaan osaamiseensa ja tietoihinsa perustuen. Myös Anderson & Agarwal (2010, 628) huomauttivat tutkimuksessaan, että käyttäytymisen muuttamisen mahdollistaa yksilön kokemus siitä, että vastatoimet ovat paitsi tehokkaita, myös hänen taitotasonsa huomioiden toteutettavissa. Voidaankin tietyllä tavalla tulkita, että aineistossa esiintyvät monenlaiset ohjeet ja paikoin hyvinkin konkreettiset neuvot ovat tarkoitettu saamaan kohdeyleisön taitotaso sellaiselle tasolle, että häneltä voidaan ylipäätään odottaa käyttäytymisen muuttamista.

Aineistossa kerrotaankin tietoturvan taitotason kehittämisestä kansalaisten keskuudessa:

> ”Toivon, että Teijo ja turvalistit sekä Pidempi parempi -salasanalinko ovat tuttuja mahdollisimman monelle. Näillä vuoden 2018 kansalaiskampanjoilla halusimme tuoda tietoturvan jokaiseen kotiin.” (Traficom 2019c)

Sitaatissa kuvaillaan kahta eri kampanjaa, jotka on tarkoitettu juuri yksityishenkilöiden tietoturvataitojen kehittämiseksi. Kuten sitaatin kirjoittaja, Kyberturvallisuuskeskuksen johtaja, kirjoittaa, tavoitteena oli tuoda tietoturva jokaisen kansalaisen luo, kotiin asti. Tämä luo kuvaa siitä, että mainittujen kampanjoiden taustalla on ollut tavoite saada aikaan laajempaa yhteiskunnallista muutosta, jossa tietoturva on jokaiselle suomalaiselle tuttua, ja kaikki suomalaiset hallitsevat tietoturvallisen käyttäytymisen. Tässä esimerkissä käyttäytymisen muutosta on pyritty edesauttamaan luomalla ihmisille mahdollisuuksia kehittää omaa tietoturvaosaamistaan sellaiselle tasolle, että toivotun käyttäytymisen toteuttaminen tulisi helpommaksi.

Kyberturvallisuuskeskuksen johtaja puhuu myös eri kohderyhmien tärkeydestä samassa aineistossa:

> ”Uskon, että ’kyberekosysteemin’ avulla sekä yksityinen että julkinen sektori pystyvät tuottamaan sellaisia sähköisiä palveluja, joita lapset, nuoret, aikuiset ja ikäihmiset voisivat käyttää tuntematta oloaan turvattomaksi.” (Traficom 2019c)

Kohderyhmien määrittelyn tärkeydestä sosiaalisen markkinoinnin kampanjoissa puhui omassa teoksessaan myös Lefebvre (2013, 52–53), jonka mukaan sosiaalisen markkinoinnin tekijöiden tulisi aina määritellä prioriteettisegmentit eli eräänlaiset pääkohderyhmät, joille kampanja on suunnattu. Tämän tutkimuksen aineisto ei edusta varsinaisesti sosiaalisen markkinoinnin kampanjamateriaaleja, vaan kyseessä on yleisistä viestinnän materiaaleista koostuva aineisto. Lisäksi Kyberturvallisuuskeskus kansallisena toimijana viestii tietoturvasta kaikille suomalaisille, jolloin kohderyhmiä tai prioriteettisegmenttejä ei pystytä samalla tavalla määrittelemään. Tämä käy ilmi myös edellisestä sitaatista: Kyberturvallisuus palvelee kaikkia suomalaisia ikään katsomatta. Näin ollen prioriteettisegmentit ja eri kohderyhmille kohdennus jäävät usein puuttumaan Kyberturvallisuuskeskuksen materiaaleista.

Kaiken kaikkiaan yhteiskunnallisen ulottuvuuden kehys sisälsi monipuolisia näkökulmia. Ensinnäkin kehykseen lukeutui muutosta käsittelevä puhe, jossa korostui ajatus siitä, että yhteiskuntien digitalisoitumisen myötä tietoturvataidot muodostuvat yhä merkittävämmäksi kansalaistaidoksi. Maailma ympärillä muuttuu nopeasti, mikä vaatii ihmisiltä mukautumista ja käyttäytymisen muuttamista tietoturvallisempaan suuntaan. Aineistossa laajempaan yhteiskunnalliseen muutokseen pyrkiminen voidaan havaita esimerkiksi tilanteissa, joissa tietoturvataitoja kuvaillaan tärkeiksi arjen kansalaistaidoiksi, tai joissa sanotaan kyberturvallisuuden kuuluvan kaikille. Yhteiskunnallisen ulottuvuuden kehyksessä viestinnän sävy vaikuttaa olevan uhkapuheen kehystä vähän kannustavampi. Siinä missä uhkapuheen kehyksessä lukijaa puhuteltiin usein sinä-muodossa, yhteiskunnallisen ulottuvuuden kehyksessä me-muoto näyttää olevan yleisempi, ja tietoturvataitoja kehitetään 'yhdessä'. Kannustavan puheen voidaan tulkita pyrkivän luomaan positiivista kuvaa tietoturvasta ja toivotusta tietoturvakäyttäytymisestä. Kuten Anderson & Agarwal (2010, 628) tutkimuksessaan totesivat, jos ihminen omaa positiivisen asenteen ehdotettuja toimia kohtaan, hän myös todennäköisemmin toimii ohjeiden mukaan, toisin kuin tilanteessa, jossa hänessä herätettäisiin vain pelkoa.

Yhteiskunnallisen ulottuvuuden kehykseen laskettiin kuuluvaksi myös sosiaaliseen markkinointiin kuuluva ajatus vaihtokaupasta ja vastavuoroisuudesta. Aineistossa vaihtokauppaa ilmeni tilanteissa, joissa kohdeyleisöä kehotettiin noudattamaan ohjeita ja neuvoja, mistä vaihtokauppana heidän tietonsa, rahallinen omaisuutensa, laitteensa tai muu vastaava pysyisi turvassa tietoturvauhilta. Kun vaihtokauppana tarjotaan jotain konkreettista, kuten juuri omien tietojensa tai rahallisen omaisuutensa koskemattomuutta, voidaan tulkita, että Rothschildin (1999, 26–27) huoli liian epämääräisistä palkinnoista pystyttäisiin välttämään. Toisaalta voidaan kuitenkin pohtia, riittävätkö nämä vaihtokauppana tarjotut asiat motivoimaan kohdeyleisöä toivottuun tietoturvakäyttäytymiseen, varsinkaan jos kohdeyleisö ei ymmärrä uhan vakavuutta ja omaa alttiuttaan uhalle. Vaihtokauppapuhetta hyödynnettiin kuitenkin aineistossa vielä suhteellisen vähän, mikä voi johtua siitä, ettei aineisto välttämättä ole laadittu alun perin sosiaalisen markkinoinnin periaatteet huomioiden. Mikäli sosiaalista markkinointia halutaan hyödyntää tietoturvaviestinnässä jatkossa, vaihtokauppapuhetta voitaisiin hyödyntää vielä enemmänkin, pitäen kuitenkin mielessä vaihtokauppana tarjottavien asioiden houkuttelevuuden.

Kuten jo todettiin, aineistoa tuskin on laadittu tietoisesti sosiaalisen markkinoinnin periaatteiden mukaan, vaikka ajatus vaihtokaupasta sekä laajempaan yhteiskunnalliseen muutokseen pyrkimisestä ovatkin aineistosta löydettävissä. Aineistosta puuttuvat kuitenkin esimerkiksi selkeät prioriteettisegmentit, jotka Lefebvre (2013) mainitsi teoksessaan tärkeänä osana sosiaalista markkinointia. Toisaalta Kyberturvallisuuskeskuksen tulee tarjota tietoa tietoturvasta kaikille suomalaisille, jolloin kohderyhmien asettaminen voi olla haastavaa. Olisi kuitenkin mahdollista pohtia, miten eri ihmisryhmät voitaisiin ottaa huomioon viestinnässä, ja pitäisikö joitain materiaaleja esimerkiksi kohdentaa erityisesti joillekin tietyille ihmisryhmille. Tehottomaksi mielletystä niin kutsutusta *one-*

size-fits-all -lähestymistavasta olisikin tutkimusten mukaan parempi siirtyä tekemään tietoturvaviestintää, joka ottaa ihmisten henkilökohtaiset ominaisuudet paremmin huomioon (ks. esim. Korpela 2015 tai Furnell & Rajendran 2012). Omanlaisestaan viestintätavasta voisivat hyötyä esimerkiksi eri ikäluokat sekä eri taitotason omaavat ihmiset unohtamatta myöskään heitä, joilla on jokin oppimisvaikeus. Lefebvren (2013) mukaan sosiaalisessa markkinoinnissa onkin tärkeää ihmiskeskeisyys ja se, mitä ihmiset tarvitsevat. Tähän erilaisten tarpeiden tunnistamiseen ja ihmiskeskeisyyteen voisikin kiinnittää huomiota tietoturvaviestinnässä, jotta tietoturvan saralla voitaisiin saada aidosti aikaan laajempaa yhteiskunnallista muutosta.

5 JOHTOPÄÄTÖKSET

Tässä tutkielmassa on tarkasteltu kansalaisille suunnattua tietoturvaviestintää erityisesti siinä esiintyvien viestinnällisten kehysten kautta. Tutkielmassa keskityttiin tietoturvaviestintään Suomen näkökulmasta, ja analyysin keskiössä olivat Suomen kansallisen tietoturvatoimijan eli Kyberturvallisuuskeskuksen tuottamat materiaalit. Tarkoituksena oli selvittää, miten yksityishenkilöille puhutaan tietoturvasta, ja minkälaista kuvaa tietoturvasta viestinnällisten kehysten avulla luodaan. Erityisesti tarkasteltiin, miten viestinnällisten kehysten avulla pyrittiin vaikuttamaan kohdeyleisön tietoturvakäyttäytymiseen. Tutkielman tutkimuskysymys kuului seuraavasti: *Miten viestinnällisten kehysten avulla pyritään vaikuttamaan ihmisten tietoturvakäyttäytymiseen yksityishenkilöille suunnatussa tietoturvaviestinnässä?*

Viestinnällisten kehysten tarkastelulla voidaan pyrkiä selvittämään, miten viestinnällä luodaan tietynlaista kuvaa todellisuudesta, ja miltä tuo todellisuus näyttää (Karvonen 2000, 78). Nämä seikat ovat puolestaan tärkeitä, koska yksityishenkilöiden tietoturvakäyttäytymisen muuttaminen edellyttää usein oikeanlaista asennetta ja oma-aloitteisuutta (Li & Siponen 2011). Siinä missä organisaatiot voivat turvautua jäsentensä velvoittamiseen toivotun tietoturvakäyttäytymisen varmistamisessa, yksityishenkilöiden tapauksessa ei ole mahdollista hyödyntää samoja menetelmiä, koska heitä ei sido mikään tietoturvapolitiikka (Li & Siponen 2011). Viestinnän on siis keksittävä muita keinoja käyttäytymiseen vaikuttamiseksi, ja kehystäminen voi olla yksi tällainen keino. Kehykset ovat olennaisia, sillä ne kertovat siitä, minkälaista kuvaa todellisuudesta luodaan. Kehysten tutkiminen onkin hyvin tärkeää käytännön kannalta viestinnän ja vaikuttamisen prosessien ymmärtämiseksi. Lisäksi tietoturvaviestinnän ja viestinnällisten kehysten tarkasteleminen on merkittävää tutkimuksen näkökulmasta, jotta voidaan selvittää, vedotaanko viestinnässä tutkimuksen valossa tarpeellisiin ja tehokkaisiin seikkoihin käyttäytymiseen vaikuttamiseksi.

Kehyksiä on tutkittu tietoturvan yhteydessä aikaisemminkin. Esimerkiksi Bada ym. (2019, 4) totesivat, että kampanjaviestit vaikuttavat tehokkaammin, jos ne on kehystetty kohdeyleisön kognitiivisten sekä tunteisiin liittyvien piirteiden mukaan. Anderson ja Agarwal (2010, 633) puolestaan jakoivat viestit po-

sitiiviin tai negatiivisiin sekä yksilötason tai yhteisötason kehyksiin. Näistä tehokkaimmin näyttää tutkijoiden mukaan vaikuttavan positiivisesti kehystetyt viestit, jotka vetoavat toivotun käyttäytymisen tarjoamiin etuihin (Anderson & Agarwal 2010). Tämän tutkielman kehykset muotoutuivat kuitenkin erilaisiksi, vaikka esimerkiksi yksilö- ja yhteisötason jaottelua voidaan nähdä myös uhkapuheen kehyksen sinä-muotoisista lauserakenteista sekä yhteiskunnallisen ulottuvuuden me-muotoiluista sekä 'yhdessä'-kielestä. Toisaalta Andersonin ja Agarwalin (2010) ajatus toivotun käyttäytymisen tarjoamiin etuihin vetoamisesta linkittyy tietyssä mielessä myös yhteiskunnallisen ulottuvuuden kehykseen ja vaihtokauppapuheeseen. Vaihtokauppapuheessa ihmiseen pyritään vetoamaan tarjoamalla käyttäytymisen muuttamisen vastineeksi jotain, kuten turvaa uhkia vastaan. Vaihtokauppa voitaisiin tietyssä mielessä mieltää eräänlaiseksi toivutun käyttäytymisen tarjoamiin etuihin vetoamiseksi, mitä Anderson ja Agarwal (2010) pitävät tehokkaana kehystämistapana. Tämä viittaa puolestaan siihen, että sosiaalisen markkinoinnin teoriaa ja käytäntöä olisi hyvä hyödyntää tietoturvaviestinnän kehystämisessä entistä enemmän jatkossa.

Tutkielma täydentää aikaisempaa tietoturvan alalla tehtyä kehystutkimusta tarkastelemalla erityisesti yhtäältä uhkiin ja pelkoon, sekä toisaalta vaihtokauppoihin sekä tietoturvataitojen välttämättömyyteen vetoamista viestinnässä luoden näin uusia lähestymistapoja ja näkökulmia. Samalla tutkielma tarjoaa lisätietoa erityisesti kampanjoita pitkäaikaisemman viestinnän tutkimukseen. Siinä missä tietoturvaan liittyvässä viestinnässä tapahtuvaa kehystämistä on aikaisemmin tutkittu lähinnä määräaikaisten kampanjoiden näkökulmasta, tässä tutkielmassa tarkasteltiin kehysten hyödyntämistä laajemmassa, pitkäaikaisessa viestinnässä, tuoden alan tutkimukseen uusia lähtökohtia ja näkökulmia. Kampanjat ovat luonteeltaan viestintää lyhytaikaisempia, ja ne keskittyvät usein johonkin tiettyyn teemaan, minkä vuoksi kampanjoiden tutkiminen ei korvaa viestinnän tutkimista laajempana kokonaisuutena. Tutkielman tarkoituksena olikin näin pyrkiä tarjoamaan lisää tietoa juuri tästä laajemmasta viestinnällisestä näkökulmasta, täydentäen näin aikaisemmassa tutkimuksessa vähemmälle huomiolle jääneitä teemoja.

Tässä tutkielmassa analyysi nojasi tietoturvatutkimuksessa erityisesti organisaatioiden kontekstissa jo laajasti hyödynnettyyn suojelumotivaatioteoriaan sekä tietoturvatutkimuksessa vähemmän käytettyyn sosiaalisen markkinoinnin teoriaan. Tutkielman voidaankin ajatella tarjoavan lisäymmärrystä suojelumotivaatioteorian soveltamisesta yksityishenkilöiden kontekstiin, mistä Li ja Siponen (2011, 7) toivoivat lisää tutkimusta. Sosiaalisen markkinoinnin teoria oli puolestaan valikoitunut mukaan tutkielmaan, koska se pystyi tarjoamaan uusia näkökulmia tietoturva-alan tutkimukseen. Näiden teorioiden pohjalta aineistosta löytyi kaksi kehystä: uhkapuheen kehys sekä yhteiskunnallisen ulottuvuuden kehys. Molempia esiintyi aineistossa määrällisesti varsin tasapuolisesti: yhteiskunnallisen ulottuvuuden kehystä esiintyi 80 kertaa ja uhkapuheen kehystä 75 kertaa.

Siinä missä uhkapuheen kehyksessä ihmisten käyttäytymiseen yritettiin vaikuttaa kuvailemalla uhkia sekä erityisesti vakuuttamalla kohdeyleisö uhan

vakavuudesta sekä omasta alttiudestaan uhille, yhteiskunnallisen ulottuvuuden kehyksessä ihmisiä kannustettiin käyttäytymisen muutokseen lupaamalla vaihtokaupaksi turvaa tietoturvauhkia vastaan. Käyttäytymisen muutoksen puolesta vedottiin yhteiskunnallisen ulottuvuuden kehyksessä myös puhumalla siitä, miten muuttuvassa yhteiskunnassa tietoturva on yhä tärkeämpi arjen kansalaistaito, jonka jokaisen tulisi hallita. Aineistossa oli havaittavissa pientä eriytymistä kehysten jakautumisessa sen perusteella, kuuluiko aineisto TTN-artikkeleihin vai Ohjeiden ja oppaiden kategoriaan. Erityisesti TTN-artikkelien joukossa esiintyi reilusti enemmän yhteiskunnallisen ulottuvuuden kehystä, kun taas Ohjeet ja oppaat -osiossa sitä esiintyi huomattavasti uhkapuhetta vähemmän. Uhkapuheen kehys puolestaan jakautui aineistossa paljon tasaisemmin. Kyberturvallisuuskeskuksessa olisikin hyvä pohtia mahdollisuutta tasapainottaa kehysten jakautumista erityisesti Ohjeiden ja oppaiden kategoriassa. Jos uhkapuheen kehys ei saa vastapainoksi yhteiskunnallisen puheen kehystä, voi vaarana olla, että ohjeet keskittyvät liikaa uhkiin ja lietsovat siten liiaksi pelkoa. Yhteiskunnallisen puheen kehystä voisikin hyödyntää entistä enemmän myös Ohjeiden ja oppaiden kategoriassa, esimerkiksi vetoamalla tietoturvaan hyödyllisenä kansalaistaitona, tai tarjoamalla toivotun tietoturvakäyttäytymisen omaksumisesta houkuttelevia, käytännönläheisiä palkintoja vaihtokauppana. Vaihtokauppaa voisi hyödyntää esimerkiksi kertomalla käytännön esimerkkejä siitä, mitä kaikkea toivotulla tietoturvakäyttäytymisellä voi suojata, ja miten elämä helpottuu jonkin tietoturvatoimen ansiosta.

Kuten mainittu, uhkapuheen kehyksessä vedotaan eniten uhan vakavuuteen, alttiuteen uhalle sekä minäpystyvyyteen, kun taas vastatoimien tehoon ja kustannuksiin sekä epätoivottua käyttäytymistä seuraaviin hyötyihin viitattiin selvästi vähemmän. Näin ollen uhkapuheessa keskitytään analyysin perusteella enemmän suojelumotivaatioteorian osa-alueeseen, jossa määritellään, miten ihminen arvioi uhkia. Tällöin analyysin perusteella vaarana on erityisesti uhkapuheen kehyksen kautta tarkasteltaessa, että viestintä saattaa herättää kohdeyleisössä jopa liiaksikin pelkoa, koska uhan vakavuus ja uhalle alttius korostuvat siinä niin paljon. Liiallinen pelko ei palvele enää tarkoitusta, minkä takia Kyberturvallisuuskeskuksen viestinnässä voitaisiinkin kiinnittää enemmän huomiota siihen, missä määrin on hyvä vedota uhan vakavuuteen tai uhalle alttiuteen, ettei se korostu liikaa. Liiallinen pelon lietsonta voi haitata käyttäytymiseen vaikuttamista, koska pelkkä pelko ei tutkimusten mukaan riitä aina motivoimaan ihmisiä haluttuun toimintaan (ks. esim. Bada ym. 2019 tai Anderson & Agarwal 2010). Uhkien kuvailun vastapainoksi tietoturvaviestinnässä olisikin hyvä vedota entistä enemmän myös suojelumotivaatioteorian toiseen osa-alueeseen, eli ihmisten arvioon kyvyistään selvitä uhista. Kyberturvallisuuskeskuksen viestinnässä voitaisiin jatkossa kehittää tasapainoa suojelumotivaatioteorian osa-alueiden välillä. Jos viestinnässä kiinnitettäisi huomiota yhä enemmän ihmisten arvioon kyvystään selviytyä uhasta, voisi se lieventää pelon syntymistä ja luoda myönteisempää asennetta. Näin Kyberturvallisuuskeskuksen viestinnän, ja tietoturvaviestinnän ylipäätään, mahdollisuudet vaikuttaa käyttäytymiseen voisivat kehittyä paremmiksi.

Yhteiskunnallisen ulottuvuuden kehyksessä esiintyvä puhe oli sävyltään uhkapuheen kehystä kannustavampaa. Tämä voidaan tulkita pyrkimyksenä luoda tietoturvasta positiivisempaa kuvaa, ja se tuo tervetullutta vastapainoa uhkapuheen kehyksen mahdollisesti luomalle pelolle. Huomionarvoista on, että selkeää vaihtokauppapuhetta esiintyi aineistossa odotettua vähemmän, mikä saattaa selittyä sillä, ettei aineistoa välttämättä ole laadittu sosiaalisen markkinoinnin lähtökohdista. Tässä onkin selkeä kehityskohta tietoturvaviestinnässä, mikäli sosiaalisen markkinoinnin teoriaa ja menetelmiä halutaan jatkossa hyödyntää. Kyberturvallisuuskeskus voisi tarjota viestinnässään entistä enemmän vaihtokauppoja, eli vedota niihin positiivisiin asioihin, joita toivotusta tietoturvakäyttäytymisestä voi seurata. Näin pystyttäisi saavuttamaan parempi tasapaino uhkapuheen lietsoman pelon kanssa, sekä luomaan oikeanlaista asennetta ja motivaatiota toivotun tietoturvakäyttäytymisen saavuttamiseksi. Erityisen tärkeää on, että tietoturvaviestinnässä vedottaisiin hyvin käytännönläheisiin vaihtokauppoihin, jolloin pystyttäisiin ottamaan huomioon myös Rothschildin (1999, 26–27) muistutus epämääräisten palkintojen välttämisestä. Näin sosiaalinen markkinointi voisi tarjota Kyberturvallisuuskeskukselle ja tietoturvaviestinnälle ylipäätään keinoja luoda vastapainoa pelon herättämiselle, kun kohdeyleisöä yritettäisi motivoida käyttäytymisen muutokseen tarjoamalla siitä vastineeksi jotain konkreettista.

Kuten edellisistä kappaleista käy ilmi, tämän tutkielman perusteella voidaan todeta, että viestinnälliset kehykset onnistuvat osittain vetoamaan suojelumotivaatioteorian sekä sosiaalisen markkinoinnin teorian valossa tarvittaviin asioihin, jos tavoitteena ajatellaan olevan vaikuttaa ihmisten käyttäytymiseen. Onnistunutta on tutkielman mukaan erityisesti suojelumotivaatioteorian mukainen vetoaminen uhan vakavuuteen, alttiuteen uhalle sekä minäpystyvyyteen, sillä näihin vedottiin aineistossa runsaasti. Kuitenkin ihmisten arvioon kyvyistään selvitä uhista vedottiin verrattaen vähän, mikä saattaa luoda epätasapainon, jolloin suojelumotivaatioteorian mukainen käyttäytymisen muuttuminen ei välttämättä tapahdu. Jos suojelumotivaatioteoriaa hyödynnetään vain osittain, se saattaa vaikuttaa lopputulokseen niin, ettei käyttäytymisen muuttamisessa onnistuta tavoitellulla tavalla. Suojelumotivaatioteoriassa molemmat osaalueet ovat tärkeitä lopputuloksen kannalta: ihmisen pitää sekä ymmärtää uhkia että pystyä arvioimaan mahdollisuuksiaan selvitä uhasta. Erityisesti jälkimmäiseen voitaisi Kyberturvallisuuskeskuksen viestinnässä vedota paljon nykyistä enemmänkin. Lisäksi sosiaalisen markkinoinnin teorian valossa vaihtokauppoihin vedottiin suhteellisen vähän. Kyberturvallisuuskeskuksen viestintä ja tietoturvaviestintä muutenkin voisi hyödyntää vaihtokauppaa ihmisiin vetoamisen keinona paljon nykyistä enemmänkin. Myös prioriteettisegmenttien määrittelyssä vaikutti aineiston perusteella olevan parantamisen varaa.

Kaiken kaikkiaan analyysin perusteella voidaan päätellä, että tietoturvasta puhutaan yksityishenkilöille paljon juuri uhkien kautta. Aineisto sisälsi runsaasti kuvauksia erilaisista uhista, niiden vakavuudesta sekä yleisyydestä. Aineistossa kerrottiin myös, miten uhkia vastaan voi yrittää suojautua. Uhat ja niiltä suojautuminen liittyivät paitsi uhkapuheen kehykseen, myös yhteiskun-

nallisen ulottuvuuden kehykseen siinä mielessä, että esimerkiksi vaihtokauppaan vedottiin usein uhkien kautta: mitä voi menettää, jos uhka realisoituu.

Erityisesti yhteiskunnallisen ulottuvuuden kehyksessä esiintyneestä 'yhdessä' tekemisen puheesta huolimatta aineistossa oli havaittavissa puutteita kohderyhmien tai prioriteettisegmenttien määrittelyissä ja niihin keskittymisessä. Toisaalta tämä on ymmärrettävää, koska Kyberturvallisuuskeskuksen tulee kansallisena tietoturvatoimijana suunnata viestintänsä kaikille suomalaisille. Kyberturvallisuuskeskuksessa voitaisiin kuitenkin pohtia, mitkä ihmisryhmät olisivat suurimman tuen tarpeessa, ja laatia jatkossa enemmän sisältöjä erityisesti heidän tarpeitaan ajatellen. *One-size-fits-all* -ajattelutavasta olisi joka tapauksessa tutkimusten mukaan hyvä siirtyä tehokkaampaan viestintään, jossa huomioidaan ihmisten eri ominaisuuksia paremmin (Korpela 2015). Yksi selkeä kehityskohta Kyberturvallisuuskeskuksen viestinnässä, ja tietoturvaviestinnässä laajemminkin, on eri kohderyhmien parempi huomioiminen. Viestintää voisikin pyrkiä kehittämään pohtimalla, pystyttäisiinkö esimerkiksi joitain materiaaleja kohdentamaan erityisesti tietyille kohderyhmille, kuten eri ikäluokille tai taitotasoille. Aiheesta voisi jatkaa myös tutkimusta tarkastelemalla esimerkiksi sitä, miten kohdeyleisö suhtautuu tietoturvaviestintään, ja miten he kokevat sen vaikuttavuuden.

Lisäksi erityisesti yhteiskunnallisen ulottuvuuden kehykseen liittyen voidaan pohtia, olivatko aineistossa tarjotut sosiaalisen markkinoinnin teoriaan liittyvät vaihtokaupat riittäviä vaikuttamaan kohdeyleisön käyttäytymiseen. Kyberturvallisuuskeskuksen viestinnässä ja tietoturvaviestinnässä yleensäkin voitaisiinkin yhä enemmän panostaa käytännönläheisten vaihtokauppojen tarjoamiseen kertomalla esimerkiksi, mitä tietoja tai omaisuutta voi pelastua toivotun tietoturvakäyttäytymisen ansiosta, tai miten elämä voi helpottua jonkin tietoturvaa edistävän toiminnan myötä. Sosiaalisen markkinoinnin hyödyntämisessä tietoturvaviestinnässä haasteeksi voi muodostua se, jos kohdeyleisö ei ymmärrä uhan vakavuutta ja omaa alttiuttaan uhalle, jolloin vaihtokauppana tarjottu turva ei välttämättä riitä motivoimaan kohdeyleisöä toivottuun käyttäytymiseen. Tämä viittaisi siihen, että suojelumotivaatioteoriaa ja sosiaalisen markkinoinnin teoriaa voitaisiin tutkielman perusteella hyödyntää yksityishenkilöille suunnatussa tietoturvaviestinnässä toisiaan täydentävinä teorioina ja keinovalikoimina. Havainto palvelee käytännön viestintää tarjoamalla uusia mahdollisuuksia viestinnän kehittämiseen, sekä tutkimusta tarjoamalla uusia sovelluksia ja lähtökohtia tietoturva-alan tutkimiseen. Tutkielma tarjoaakin uudenlaisen lähtökohdan tietoturvatutkimukseen pohjustamalla sosiaalisen markkinoinnin käyttöä tietoturva-alan kontekstissa. Suojelumotivaatioteoriaa ja sosiaalista markkinointia yhdisteltäessä olisi erityisesti käytännön näkökulmasta mahdollista myös huomioida Andersonin & Agarwalin (2010, 628) muistutus, ettei pelko yksinään riitä saamaan ihmistä toimimaan tietyllä tavalla, vaan ihmisillä tulisi olla myös positiivinen asenne vastatoimia kohtaan.

Tietoturvaviestintää voisikin tulevaisuudessa tarkastella eri tutkimuksissa lisää juuri sosiaalisen markkinoinnin kautta. Tietoturva vaikuttaa lisäksi tutkimuksen perusteella sellaiselta alalta, johon sosiaalista markkinointia voisi hyö-

dyntää yhä enemmän myös käytännössä, sillä tietoturvan yhteiskunnallinen merkitys tuskin ainakaan vähenee. Tietoturvaosaamisen tarve yhteiskunnassa kasvanee yhä tulevaisuudessa, jolloin tarve laajemmalle yhteiskunnalliselle muutokselle kohti tietoturvallisempaa, ja tietoturvaosaamiseltaan parempaa, yhteiskuntaa voisi perustella sosiaalisen markkinoinnin hyödyntämisen tässä yhteydessä. Joissain tutkimuksissa on myös havaittu, että positiivisuus ja kannustaminen motivoisivat käyttäytymisen muuttamiseen parhaiten (ks. esim. Anderson & Agarwal 2010). Sosiaalinen markkinointi voisi auttaa tässä.

Tutkimusasetelman takia analyysin ja sen myötä koko tutkielman ulkopuolelle on saattanut jäädä joitain näkökulmia. Koska analyysissa käytettiin deduktiivista kehysanalyysitapaa, jossa alustavasti määritellyt kehykset johdattelivat analyysiprosessia, aineistosta voisi periaatteessa olla löydettävissä erilaisiakin kehyksiä, jos lähestymistapa olisi induktiivinen. Deduktiivisella analyysitavalla pyrittiin parantamaan tutkimuksen toistettavuutta, ja tutkimalla tulevaisuudessa vastaavaa aihetta lisää on mahdollista saavuttaa vieläkin laajempi ymmärrys aiheesta. Vaikka esimerkiksi deduktiivisella lähestymistavalla on pyritty minimoimaan tutkimuksen reliabiliteettiin ja validiteettiin liittyviä kysymyksiä, on huomioitava, että kehysanalyysin sidosteisuutta tekijäänsä on menetelmän luonteen vuoksi vaikeaa täysin välttää. Tämän takia olisikin hyvä saada tulevaisuudessa lisää kehysanalyyttista tutkimusta tietoturvaviestinnästä eri tutkijoiden tekemänä.

Tutkielman haasteisiin lukeutui myös se, miten tietoturvaviestintää on tutkittu enemmän kampanjoiden näkökulmasta, mikä toi omat haasteensa tutkimusasetelman luomiseen. Esimerkiksi teoreettisen viitekehyksen luomisessa oli hyödynnettävä tietoturvakampanjoita koskevaa tutkimuskirjallisuutta pitkäaikaisempaa viestintää koskevan tutkimuksen vähyyden vuoksi. Olisikin kiinnostavaa nähdä jatkossa lisää tutkimusta tietoturvaviestinnästä myös kampanjoita laajemmasta näkökulmasta. Tämän tutkielman tieteellinen merkitys kulminoituukin lähtökohtien ja näkökulmien tarjoamiseen tulevalle tietoturvaviestinnän tutkimukselle, erityisesti kehysanalyyttisille lähestymistavoille. Lisäksi tutkielman tieteellisenä arvona voidaan nähdä kampanjoita laajempaa tietoturvaviestintää tarkastelevien tulevien tutkimusten pohjustaminen. Myös sosiaalisen markkinoinnin teorian hyödyntäminen tietoturva-alan tutkimuksessa on ollut aikaisemmin vähäistä, mikä tarjosi haasteita analyysiin. Tutkielman aineisto ei välttämättä ollut sosiaalisen markkinoinnin näkökulmasta paras mahdollinen, koska se ei liene laadittu alun perin sosiaalisen markkinoinnin periaatteet huomioiden. Sosiaalisen markkinoinnin luomia viestinnällisiä mahdollisuuksia voitaisiin pohtia jatkossa enemmän myös käytännössä, mihin tämä tutkielma voikin tarjota eväitä. Lisäksi tutkielma voi tarjota pohjustusta ja lähtökohtia myös tuleville sosiaalisen markkinoinnin ja tietoturvan yhdistäville mittavammille tutkimuksille.

Kaiken kaikkiaan yksityishenkilöille suunnatussa tietoturvaviestinnässä on eri teorioiden ja tutkimusten mukaan monia mahdollisia kompastuskiviä. Yhtäältä pieni pelko voi motivoida ihmistä muuttamaan käyttäytymistään, toisaalta pelko voi lamauttaa tai saada ihmisen uskottelemaan itselleen, ettei uhka

ole oikeasti niin vaarallinen, tai ettei se oikeastaan koske juuri häntä. Tämä on viestinnälle iso haaste, minkä takia on tärkeää, että tietoturvaviestintää tutkitaan ja ymmärretään entistä paremmin. Tutkimuksella on myös tärkeä rooli käytännön työn kehittämisessä.

Tietoturvasta yksityishenkilöille viestivien haasteena on myös tietynlainen auktoriteetin puute. Organisaatioiden jäseniä sitoo usein organisaation tietoturvapolitiikka, joka määrittelee toivotun ja epätoivotun käyttäytymisen rajat, mutta yksityishenkilöille mitään vastaavaa sitovaa ohjeistusta ei ole (Li & Siponen 2011). Yksityishenkilöille on kuitenkin tarjolla tietoa toivotusta tietoturvakäyttäytymisestä sekä neuvoja sen toteuttamiseen. Haasteeksi jää, miten yksityishenkilöt ensinnäkin saadaan ohjeiden pariin, ja toiseksi noudattamaan niitä, koska yksityishenkilöille ohjeiden noudattaminen on vapaaehtoista. Näihin haasteisiin voitaisiin yrittää vastata juuri suojelumotivaatioteorian sekä sosiaalinen markkinoinnin avulla. Tietoturvaviestintää voitaisiin kehittää erityisesti keskittymällä entistä enemmän tiettyihin kohderyhmiin sekä tarjoamalla enemmän houkuttelevia, käytännönläheisiä palkintoja vaihtokauppana. Lisäksi tietoturvaviestintää voitaisiin kehittää vetoamalla yhä enemmän ihmisten arvioon kyvyistään selvitä uhasta, ja välttämällä liiallista pelon lietsomista korostamalla nykyistä vähemmän uhkien vakavuutta sekä uhille alttiutta. Viestinnän sävyihin ja viestien kehystämiseen on hyvä kiinnittää erityistä huomiota jatkossakin, koska näiden avulla viestintä voi pyrkiä vaikuttamaan ihmisten käyttäytymiseen. Toisaalta jos viestintä epäonnistuu kehystämisessä, voi se pahimmillaan estää viestinnän vaikuttamistavoitteiden täyttymisen.

Tämän tutkielman tavoitteena oli lisätä ymmärrystä yksityishenkilöille suunnatusta tietoturvaviestinnästä erityisesti viestinnässä hyödynnettyjen kehysten tunnistamisen kautta. Kehysten tunnistaminen mahdollistaa niiden tarkoituksenmukaisuuden arvioinnin, sekä niiden johdonmukaisemman tietoisen hyödyntämisen jatkossa. Kuten Kyberturvallisuuskeskuksen viestintämateriaaleissakin monesti sanottiin, yhteiskunta muuttuu kovaa vauhtia suuntaan, jossa tietoturva on yhä merkittävämpää myös tavallisille kansalaisille. Yksityishenkilöille suunnatun tietoturvaviestinnän ja heidän tietoturvatietoisuutensa kehittämisen tarve kasvanee tulevaisuudessa. Näin ollen yksityishenkilöille suunnatun tietoturvaviestinnän tutkiminen on mielekästä myös jatkossa, jopa enenemässä määrin.

LÄHTEET

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & information technology, 33(3), 237-248. doi:10.1080/0144929X.2012.708787

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions.(Report). MIS Quarterly, 34(3), 613-643. doi:10.2307/25750694

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? Ithaca: Cornell University Library, arXiv.org.

D'Arcy, J., Hovav, A. & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research, 20(1), 79-98, 155, 157. https://doi.org/10.1287/isre.1070.0160

Dahl, S., Eagle, L. & Ebrahimjee, M. (2013). Golden Moves: Developing a Transtheoretical Model-Based Social Marketing Intervention in an Elderly Population. Social marketing quarterly, 19(4), 230-241. https://doi.org/10.1177/1524500413505569

Dolan, P., Hallsworth, M., Halpern, D., King, D., Metcalfe, R. & Vlaev, I. (2012). Influencing behaviour: The mindspace way. Journal of economic psychology, 33(1), 264-277. doi:10.1016/j.joep.2011.10.009

Entman, R. (1993). Framing: Toward clarification of a fractured paradigm. Journal of Communication, 43(4), 51-58. https://doi.org/10.1111/j.1460-2466.1993.tb01304.x

Floyd, D., Prentice-Dunn, S. & Rogers, R. (2000). A meta-analysis of research on protection motivation theory. Journal Of Applied Social Psychology, 30(2), 407-429.

Furnell, S., Bryant, P. & Phippen, A. (2007). Assessing the security perceptions of personal Internet users. Computers & Security, 26(5), 410-417. doi:10.1016/j.cose.2007.03.001

Furnell, S. & Rajendran, A. (2012). Understanding the influences on information security behaviour. Computer fraud & security, 2012(3), 12-15. doi:10.1016/S1361-3723(12)70053-2

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. Computers & security, 73, 345-358. doi:10.1016/j.cose.2017.11.015

Hastings, G. (2007). Social marketing: Why should the Devil have all the best tunes?

Ikäheimo, H. (2016). EU nautintovarkaana: Tulkintakehykset ”EU kieltää” -artikkeleissa. Politiikka 58(4), 263–279.

Kajzer, M., D'Arcy, J., Crowell, C. R., Striegel, A. & Van Bruggen, D. (2014). An exploratory investigation of message-person congruence in information security awareness campaigns. Computers & Security, 43, 64-76. https://doi.org/10.1016/j.cose.2014.03.003.

Karvonen, E. (2000). Tulkintakehys (frame) ja kehystäminen. Tiedotustutkimus 23(2), 78–84.

Korpela, K. (2015). Improving Cyber Security Awareness and Training Programs with Data Analytics. Information security journal., 24(1-3), 72-77. doi:10.1080/19393555.2015.1051676

Kortjan, N. & Von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA: Research article. South African Computer Journal (SACJ) No 52. 29-41. DOI: https://doi.org/10.18489/sacj.v52i0.201

Korzaan, M. L. & Boswell, K. T. (2008). The Influence of Personality Traits and Information Privacy Concerns on Behavioral Intentions. The Journal of computer information systems, 48(4), 15-24. doi:10.1080/08874417.2008.11646031

LaRose, R., Rifon, N. & Enbody, R. (2008). Promoting personal responsibility for internet safety. Communications of the ACM, 51(3), 71-76. doi:10.1145/1325555.1325569

Lefebvre, R. C. (2013). Social marketing and social change: Strategies and tools for health, well-being, and the environment. Jossey-Bass.

Li, Y. & Siponen, M. (2011). A call for research on home users information security behaviour. In: PACIS 2011, Proceedings (paper 112).

Menard, P., Bott, G. J. & Crossler, R. E. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-

Determination Theory. Journal of management information systems, 34(4), 1203-1230. https://doi.org/10.1080/07421222.2017.1394083

Nurmi, T., Rekiaho, I. & Rekiaho, P. (2009). Uusi suomen kielen sivistyssanakirja. Jyväskylä: Gummerus.

Pahnila, S., Siponen, M. & Mahmood A. (2007). Employees' Behavior towards IS Security Policy Compliance. 40th Annual Hawaii International Conference on System Sciences (HICSS'07). doi: 10.1109/HICSS.2007.206.

Prochaska, J. O. & DiClemente, C. C. (1982). Transtheoretical therapy: Toward a more integrative model of change. Psychotherapy: Theory, Research & Practice, 19(3), 276-288. https://doi.org/10.1037/h0088437

Puhakainen, P. & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. Mis Quarterly, 34(4), 757-778.

Rogers, E. M. (2003). Diffusion of innovations (Fifth edition.). Free Press.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. The Journal of Psychology, 91(1), 93-114. doi:10.1080/00223980.1975.9915803

Rothschild, M. (1999). Carrots, Sticks, and Promises: A Conceptual Framework for the Management of Public Health and Social Issue Behaviors. Journal of Marketing, 63(4), 24-37. https://doi.org/10.2307/1251972

Sarkin, J. A., Johnson, S. S., Prochaska, J. O. & Prochaska, J. M. (2001). Applying the Transtheoretical Model to Regular Moderate Exercise in an Overweight Population: Validation of a Stages of Change Measure. Preventive medicine, 33(5), 462-469. https://doi.org/10.1006/pmed.2001.0916

Shaw, R., Chen, C. C., Harris, A. L. & Huang, H. (2009). The impact of information richness on information security awareness training effectiveness. Computers and education, 52(1), 92-100. doi:10.1016/j.compedu.2008.06.011

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31-41. https://doi.org/10.1108/09685220010371394

Siponen, M. & Vance, A. (2010). Neutralization: New Insights Into The Problem Of Employee Information Systems Security Policy Violations. MIS Quarterly, 34(3), 487-A12. doi:10.2307/25750688

Siponen, M. & Vance, A. (2012). IS Security Policy Violations: A Rational Choice Perspective. Journal of Organizational and End User Computing 24(1), 21-41. doi.org/10.4018/joeuc.2012010102

Straub, D. (1990). Effective IS Security: An Empirical Study. Information Systems Research, 1(3), 255-276. doi:10.1287/isre.1.3.255

Tanner, J., Hunt, J. & Eppright, D. (1991). The Protection Motivation Model: A Normative Model of Fear Appeals. Journal of Marketing, 55(3), 36-45. https://doi.org/10.2307/1252146

Vance, A., Siponen, M. & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49(3-4), 190-198. doi:10.1016/j.im.2012.04.002

De Vreese, C. (2005). News framing: Theory and typology. Information Design Journal, 13(1), 51–62. https://doi.org/10.1075/idjdd.13.1.06vre

LIITE 1: AINEISTO

Traficom 2019a: TOP 5 tietoturvauhat ja -ratkaisut yksityishenkilöille, julkaistu 17.01.2019, katsottu 25.5.2021, saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/top-5-tietoturvauhat-ja-ratkaisut-yksityishenkiloille
Traficom 2019b: 10 + 1 näkymää tietoturvan vuodelle 2019, julkaistu 30.01.2019, katsottu 25.5.2021, saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/10-1-nakymaa-tietoturvan-vuodelle-2019
Traficom 2019c: Kyberturvallisuus kuuluu kaikille, allekirjoitus päivätty 31.01.2019, katsottu 25.5.2021, saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuus-kuuluu-kaikille
Traficom 2019d: Tunnista, suojaudu ja torppaa nettihuijarin aikeet, julkaistu 02.05.2019, katsottu 25.5.2021, saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tunnista-suojaudu-ja-torppaa-nettihuijarin-aikeet
Traficom 2019e: Nasevia neuvoja tiliesi turvaamiseksi, julkaistu 04.09.2019 (päivitetty 30.10.2020), katsottu 25.5.2021, saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/nasevia-neuvoja-tiliesi-turvaamiseksi
Traficom 2019f: Hallitsetko nämä tietoturvan perustaidot? Julkaistu 12.09.2019, katsottu 25.5.2021, saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/hallitsetko-nama-tietoturvan-perustaidot
Traficom 2019g: Turvalisti-Teijo on mukana Euroopan kyberturvallisuuskuukaudessa, julkaistu 09.10.2019, katsottu 25.5.2021, saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/turvalisti-teijo-mukana-euroopan-kyberturvallisuuskuukaudessa
Traficom 2019h: Suomi aloittaa älylaitteiden turvallisuuden varmistamisen ensimmäisenä Euroopassa – uusi Tietoturvamerkki auttaa kuluttajia tekemään turvallisempia kodin älylaitehankintoja, julkaistu 26.11.2019, katsottu 25.5.2021, saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/suomi-aloittaa-alylaitteiden-turvallisuuden-varmistamisen-ensimmaisena-euroopassa
Traficom 2020a: Yhteiskuntamme haavoittuvuuksia ei korjata vain keskustelemalla, julkaistu 09.01.2020 (päivitetty 18.02.2020), katsottu 25.5.2021, saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/yhteiskuntamme-haavoittuvuuksia-ei-korjata-vain-keskustelemalla
Traficom 2020b: Tietoturvan selviytymispakki koteihin ja toimistoihin – 3 uhkaa ja ratkaisua, julkaistu 17.01.2020, katsottu 25.5.2021, saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvan-selviytymispakki-koteihin-ja-toimistoihin-3-uhkaa-ja-ratkaisua

Traficom 2020c: 10 tietoturvanäkymää vuodelle 2020, julkaistu 22.01.2020, katsottu 25.5.2021, saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/10-tietoturvanakymaa-vuodelle-2020
Traficom 2020d: Yhteiskunta tarvitsee tietoturvallisia arjen tekoja – yhdessä olemme vahvin lenkki, allekirjoitus päivätty 19.02.2020, katsottu 25.5.2021, saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvan-vuosi-2019-sisalsi-iloa-murhetta-ja-muutoksia
Traficom 2020e: Netiketti – Verkossa liikkujan työkalupakki. Päivätty 30.04.2020, katsottu 25.5.2021. Saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/netiketti-verkossa-liikkujan-tyokalupakki
Traficom 2020f: Neuvoja epäilyttävien sivujen tunnistamiseksi, julkaistu 07.05.2020, katsottu 25.5.2021, saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-epailyttavien-sivujen-tunnistamiseksi
Traficom 2020g: Näin suojaudut tietomurroilta. Päivätty 21.07.2020, katsottu 25.5.2021. Saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-tietomurroilta
Traficom 2020h: Näin pidät huolta tietoturvasta kotona ja työpaikalla. Päivätty 21.07.2020. katsottu 25.5.2021, Saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-pidat-huolta-tietoturvasta-kotona-ja-tyopaikalla
Traficom 2020i: Turvallisuusopas poikkeusolojen jälkeiseen aikaan. Päivätty 13.08.2020. katsottu 25.5.2021, Saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/turvallisuusopas-poikkeusolojen-jalkeiseen-aikaan
Traficom 2020j: Pidempi parempi – Näin teet hyvän salasanan. Päivätty 28.08.2020. katsottu 25.5.2021, Saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/pidempi-parempi-nain-teet-hyvan-salasanan
Traficom 2020k: #tietoturvatorstai - Ota arjen tietoturva haltuun asiantuntijoidemme kanssa, julkaistu 17.09.2020, katsottu 25.5.2021, saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvatorstai-ota-arjen-tietoturva-haltuun-asiantuntijoidemme-kanssa
Traficom 2020l: Kyberturvallisuuden superkuukausi on täällä taas! Julkaistu 01.10.2020, katsottu 25.5.2021, saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuden-superkuukausi-taalla-taas
Traficom 2020m: Kotiturvalistit – Äly-TV. Julkaistu 11.12.2020, katsottu 25.5.2021, saatavilla: https://youtu.be/CLWa0XLiaUA
Traficom 2020n: Kotiturvalistit – Salasana. Julkaistu 11.12.2020, katsottu 25.5.2021, saatavilla: https://youtu.be/OvqPLLDkoxI

Traficom 2020o: Kotiturvalistit – Päivitykset. Julkaistu 11.12.2020, katsottu 25.5.2021, saatavilla: https://youtu.be/6JCvriWda_4
Traficom 2021a: 10 tietoturvanäkymää vuodelle 2021, julkaistu 20.01.2021, katsottu 25.5.2021, saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/10-tietoturvanakymaa-vuodelle-2021
Traficom 2021b: Näin suojaudut nettihuijaukselta. Päivätty 02.02.2021, katsottu 25.5.2021. Saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-nettihuijaukselta
Traficom 2021c: Tietoturva 2021: 3 uhkaa ja 3 ratkaisua jokaiselle, Julkaistu 04.02.2021, katsottu 25.5.2021, saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturva-2021-3-uhkaa-ja-3-ratkaisua-jokaiselle
Traficom 2021d: Salasanat haltuun – Kuka käyttää tiliäsi? Päivätty 25.03.2021, katsottu 25.5.2021. Saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/salasanat-haltuun

LIITE 2: VIDEOIDEN LITTERAATIT

Kotiturvalistit – Äly-TV (julkaisija: Liikenne- ja viestintävirasto Traficom, julkaistu 11.12.2020, katsottu 25.5.2021. Saatavilla: https://youtu.be/CLWa0XLiaUA)

Kertoja: Kodissasi piilee älykkyyttä, ehkä enemmän kuin olet tullut ajatelleeksikaan.

Henkilö1: Mieti jos joku pystyisi katselemaan tuolta telkkarista tänne meille. Eikö nykypäivänä hakkerit pysty tunkeutumaan mihin tahansa älylaitteisiin?

H2: Nii ja sit ne näkisi, kuinka paljon mä oon tänään syönyt.
H1: Ja ne näkisivät ne kanavat, mitä me ollaan katseltu.

K: Käytä älylaitteitasi tietoturvallisesti. Näin tukit rikollisen väylät laitteisiisi, ja olet itse - myös äly-tv:si - valtias.

H2: Pitäisikö jääkaappeihinkin laittaa salasana?
H1: Niissähän on jo. Oikeasti!

K: Niinpä. Älylaitteesi on kuin tietokone - se on yhteydessä nettiin. Ota siis selvää sen tietoturvasta. Esimerkiksi salasanan vaihtaminen ja päivitysten lataaminen kodin älylaitteisiin onnistuu myös sinulta. Se on paras tapa pitää kaiken maailman hakkerit loitolla. Ole sinäkin Kotiturvalisti! Tutustu myös Tietoturvamerkkiin, se kertoo, että älylaitteen tietoturva on kunnossa.

Kotiturvalistit – Salasana (julkaisija: Liikenne- ja viestintävirasto Traficom, julkaistu 11.12.2020, katsottu 25.5.2021. Saatavilla: https://youtu.be/OvqPLLDkoxI)

Kertoja: Eijan sähköpostitilille on kirjauduttu ulkomailta, vaikka kukaan heistä ei ole käynyt Lohjaa kauempana kokonaiseen vuoteen.

Eija: Täällä lukee. Täällä lukee, että minun sähköpostiini on kirjauduttu uudella laitteella Lontoossa.
Mies: Lontoosta?
E: Nii.
Tytär: Ootko sä taas klikannut jotain outoa linkkiä?
E: Yhteen arvontaan joskus osallistuin.
M: Noni

K: Hei! Olet saattanut joutua tietojenkalastelijan saaliiksi.

T: Äiti, nyt kuule vaihdetaan sun salasana. Nythän sitä voi käyttää sit kuka vaan, jos se on…
E: Nii…
T: No vaihdetaan saman tien. Laita joku hyvä, ja joku minkä muistat.

K: Käyttäjätunnukset ja salasanat ovat kovaa valuuttaa hakkeripiireissä. Niitä siis myydään. Hyvä salasana on pitkä ja vain sinun tiedossasi. Ja pituutta saat helposti, jos kasaat sanoista lauseen.

E: Noin.
T: Pitäisikö siihen kerralla laittaa tommonen monivaiheinen tunnistautuminen?
E: No, mikäs se on?
T: No siis se on semmonen, että sen lisäksi kun sä laitat sinne ton salasanan, nii sen lisäks sulle tulee toinen tunnistautumisvaihe. Sä saat koodin tekstiviestillä sun kännykkään. Ja se on joka kerta aina eri, uus koodi. Joka kerran kun sä meet tonne sisään.
M: Monimutkainen.
T: Ei kun monivaiheinen. Voilà!
E: Nyt se tuli jo.
T: Niin tuli.
E: No eihän tämä nyt ollut niin hankalaa.

K: Eipä. Monivaiheinen tunnistautuminen ei todellakaan ole hankalaa. Ja se on varma tapa pitää kaiken maailman tietojenkalastelijat kurissa.

Kotiturvalistit – Päivitykset (julkaisija: Liikenne- ja viestintävirasto Traficom, julkaistu 11.12.2020, katsottu 25.5.2021. Saatavilla: https://youtu.be/6JCvriWda_4)

Kertoja: Onko tablettisi ja kännykkäsi päivitetty? Toivottavasti, koska päivittämätön älylaite on altis häkkereiden hyökkäyksille.

Lapsi: Äiti, tää peli ei lataudu.
Äiti: Mikä?
L: No tää yks peli.
Ä: No mikä ikäraja siin on?
L: 12.
Ä: Ja mitä se maksaa?
L: Ihan sikavähän.
Ä: No joo, on se aika halpa. Mut mikä tää niin kuin on?
L: Tää on sellanen tosi hyvä peli, jota mun kaikki kaverit pelaa.

K: Hei! Pelin lataaminen ei välttämättä onnistu, jos tabletin käyttöjärjestelmän uusinta päivitystä ei ole tehty.

Ä: Siis kannattaa päivittää se, ettei kukaan pääse häkkään tuota.
L: Mä en halua mitään häkkäystä, mä haluisin vain pelata. Mut miten se tehtiin?
Ä: Valitse tuo.
L: Tää päivittää tän automaattisesti! Mä valitsen ton ja se lataa sen uusimman version.
Ä: Joo, no nyt siinä sit menee muutama minuutti. Pärjäätkö sen aikaa ilman tablettia?
L: Muuten, tiedätkö mitä muuta voisi päivittää?
Ä: Noh?
L: Sun tukkatyyli, ja sitten sun vaatekaappi, sun passikuva, ja sit mun viikkorahat.
Ä: Vai niin, vai niin.

K: Niinpä. Päivittäminen kannattaa lähes aina. Se on myös paras tapa pitää kodin digilaitteet toimivina ja tietoturvallisina.

L: Pitäisikö teilläkin vähän päivittää?