SaaS-organisaatioiden luotettavuus kyberympäristössä – ”Siellä on se teknologia ja sitten on myös ihminen.”

Jyväskylän yliopisto
Kauppakorkeakoulu

Pro gradu -tutkielma

2018

Tekijä: Mervi Väisänen
Oppiaine: Viestinnän johtaminen
Ohjaaja: Outi Ihanainen-Rokio

JYVÄSKYLÄN YLIOPISTO

TIIVISTELMÄ

<table>
<tr><td>Tiedekunta – Faculty
Kauppakorkeakoulu</td><td>Laitos – Department
Viestinnän johtaminen</td></tr>
<tr><td colspan="2">Tekijä – Author
Väisänen, Mervi</td></tr>
<tr><td colspan="2">Työn nimi – Title
SaaS-organisaatioiden luotettavuus kyberympäristössä –”Siellä on se teknologia ja sitten on myös ihminen.”</td></tr>
<tr><td>Oppiaine – Subject
Viestinnän johtaminen</td><td>Työn laji – Level
Maisterintutkielma</td></tr>
<tr><td>Aika – Month and year
Syyskuu 2018</td><td>Sivumäärä – Number of pages
66+5</td></tr>
<tr><td colspan="2">Tiivistelmä – Abstract
Tärkeintä kyberturvallisuusuhkia vastaan on organisaation luotettavuuden rakentaminen, joka on myös yksi organisaatioviestinnän tehtävistä. Kyberiskujen keinot ja määrä kasvavat koko ajan, joten talous, luottamus ja maine voivat olla vaakalaudalla. Pilvipalveluita tarjoavat SaaS-organisaatiot ovat erityisen alttiita luotettavuuden ja maineen menetykselle, koska liiketoiminta perustuu täysin kyberympäristöön.

Tutkimuksessa haluttiin selvittää: 1) Miten kyberturvallisuusuhkat liittyvät SaaS-organisaatioiden luotettavuuteen ja maineeseen ja 2) Miten viestinnällä voidaan vaikuttaa organisaation luotettavuuteen kyberympäristössä. Tutkimusaineisto hankittiin teemahaastatteluilla kahdeksasta SaaS-palveluita tuottavasta organisaatiosta. Analysointi toteutettiin aineistolähtöisellä analyysillä.

Tulosten mukaan useissa SaaS-organisaatioissa ei nähty kyberturvallisuusuhkien aiheuttavan maine- ja luotettavuusriskejä. Kyberturvallisuusuhkia pidettiin organisaation sisäisenä asiana ja ulkoisille sidosryhmille viestiminen nähtiin jopa tarpeettomana. Luotettavuutta ja kyberturvallisuutta rakennettiin mm. sidosryhmälähtöisellä ja monipuolisella organisaatioviestinnällä, mutta aito vuorovaikutus ulkoisten sidosryhmien kanssa puuttui ja viestintä oli lähinnä tiedon jakamista. Lisäksi kyberturvallisuutta koskeva ulkoinen viestintä ja yhteistyö puuttuivat usein kokonaan.

Mielenkiintoisia jatkotutkimusaiheita voisivat olla mm. kyberturvallisuusuhkien merkitys luotettavuuteen muilla toimialoilla ja kyberturvallisuusuhkien huomioiminen riski- ja kriisiviestintäsuunnitelmissa.</td></tr>
<tr><td colspan="2">Asiasanat – Keywords
Kyberturvallisuus, luotettavuus, luottamus, maine, organisaatioviestintä, SaaS, toimijaverkkoteoria.</td></tr>
<tr><td colspan="2">Säilytyspaikka – Depository
Jyväskylän yliopiston kauppakorkeakoulu</td></tr>
</table>

SISÄLLYS

TAULUKOT

KAAVIOT

1 JOHDANTO

Marraskuussa 2017 uutisoitiin, kuinka Uber, taksiliikennettä kansainvälisesti harjoittava yhdysvaltalainen yritys, oli maksanut hakkereille 100 000 dollaria eli yli 85 000 euroa saadakseen hakkerit tuhoamaan varastamansa Uberin 50 miljoonan asiakkaan ja seitsemän miljoonan ajajan yksityistiedot. Uutisen mielenkiinto ei ollut niinkään suuressa rahasummassa vaan erityisesti siinä, että yritys oli pyrkinyt salaamaan tietojen varastamisen. Tiedot oli hakkeroitu yrityksestä jo vuonna 2016 ja vasta vuoden jälkeen tapahtuneesta Uber tuli asian kanssa julkisuuteen. (Bloomberg 21.11.2017; Yle 22.11.2017).

Kyberturvallisuusuhkien toteutuessa organisaatiot voivat kärsiä taloudellisten menetysten lisäksi maineriskistä ja luottamuksen menetyksestä (Peltonen ja Norppa 2015, 98). Uberin entinen toimitusjohtaja päätti salata tietomurron ja voidaan vain epäillä, olisiko salailun syynä ollut pelko maineen tahraantumisesta ja luotettavuuden menetyksestä.

Limnéll, Majewski ja Salminen (2014, 24-25) toteavat, että luottamus on yksi tärkeimmistä turvallisuutta luovista tekijöistä kyberympäristössä. Organisaatioiden sidosryhmät luottavat, että heidän tietonsa ovat turvassa, mutta he myös luottavat siihen, että organisaatiosta annettu tieto on luotettavaa. Näin uskoi elokuussa 2017 myös osa suomalaisista, kun he saivat Verohallinnolta sähköpostia, jossa ilmoitettiin sähköpostin saajalle olevan tulossa veronpalautuksia. Veronpalautusten saamiseksi henkilön tuli kirjautua verkkopankkiin sähköpostissa olevasta linkistä. Kyse oli kuitenkin tietojenkalasteluviestistä, jossa tarkoituksena oli saada asiakkaiden pankkitunnukset väärin käsiin. (Viestintävirasto verkkotiedote 7.9.2017).

Yllä mainituissa esimerkeissä on kyse ollut hakkeroinnista organisaation järjestelmään ja sähköpostihuijauksesta. Nykyisin kyberiskuja voidaan tehdä kuitenkin myös matkapuhelimiin tekstiviesteillä (Viestintävirasto julkaisu 001/2018, 6) niissä olevien sovellusten kautta. Esimerkiksi Lidl tiedotti kotisivuillaan 12.1.2018, että sen nimissä leviää WhatsApp -sovelluksessa huijausviesti, jossa suositellaan osallistumaan 250 euron lahjakortin arvontaan (Lidl, verkkosivut 2018).

Vaikka näissä tapauksissa kyse on isoista organisaatioista, ei voida sanoa, että kukaan tai mikään organisaatio olisi turvassa kyberuhilta. ”*Tuoreiden arvioiden mukaan verkossa tapahtuu jopa miljardeja hyökkäyksiä ja hyökkäykseen tähtääviä toimenpiteitä sekunnissa. Ne aiheuttavat satojen miljardien eurojen taloudelliset menetykset vuodessa*”, sanoi Oulun yliopiston informaatioteknologin dosentti Tapio Frantti Ylen (28.9.2017) haastattelussa.

Tapio Frantin mainitsemat määrät tietoturvaloukkauksista ja niihin tähtäävistä teoista ovat valtavia. Kukaan yksittäinen ihminen, saati organisaatio ei voi sanoa olevansa täysin turvassa hyökkäyksiltä tai niiden uhkilta. Uhkien ja iskujen lisääntyminen sekä toteutustapojen monipuolistuminen ovat varmasti osa syy siihen, että kyberhyökkäyksistä on puhuttu varsinkin parin viime vuoden aikana enenevissä määrin. Uutiset ja tutkimukset ovat silti keskittyneet tietojärjestelmiin ja niiden turvallisuuteen, eivät organisaatioiden maineriskeihin tai luotettavuuden menetykseen. Kyberturvallisuus nähdään enemmän teknisenä asiana, toteavat Limnéll ym. (2014, 13). Lisäksi ongelma on, että jos kyberhyökkäyksistä ei puhuta, johtaa se vääristyneeseen kuvaan turvallisuudesta, eli turvallisuutta pidetään parempana mitä se on (Limnéll ym. 2014, 82-83).

Maine ja luottamus ovat kuitenkin tärkeitä asioita, sillä esimerkiksi MacMillanin ja muiden (2005, 228) tekemän tutkimuksen mukaan luottamus vaikuttaa mm. sidosryhmien uskollisuuteen, sitoutumiseen, organisaation suositteluun muille ja myös siihen, haluavatko he vahingoittaa organisaatiota. Maister, Green ja Galford (2012, 48) tuovat puolestaan esille, että luottamus vaatii aikaa ja pitkäjänteisyyttä. Aula ja Heinonen (2002, 60) sanovat, että *"maine on luottamusta"*. Koska luottamuksen ja sitä kautta maineen takaisinsaaminen ei ole varmaa, kannattaa organisaation pyrkiä varmistamaan, että kolhuja tulisi mahdollisimman vähän. Erinomainen keino kyberturvallisuusuhkiin liittyvään maineenhallintaan on avoimuus, läpinäkyvyys ja yhteistyö (Limnéll ym. 2014, 83) ja näihin organisaatioviestinnällä on mahdollisuus vaikuttaa.

1.1 Tutkimuksen tavoite ja aiheen valinta

Kyberturvallisuusuhkia ja viestintää yhdistävälle tutkimukselle voidaan katsoa olevan tarve, sillä "verkkomaineen" merkitys korostuu tulevaisuudessa entisestään ja varsinkin niillä yrityksillä, jotka toimivat vain internetissä (Peltonen ja Norppa 2015, 132). Lisäksi kyberhyökkäysten määrä organisaatioita kohtaan on lisääntynyt (Viestintävirasto 2018, 6). Kendrickin (2010, 23, 37) mukaan organisaatioiden on oltava verkossa avoimia, luotettavia ja läpinäkyviä kaikkia sidosryhmiä kohtaan ja luottamus on yksi tärkeimmistä tekijöistä sidosryhmäsuhteissa (Aula ja Mantere 2005, 166).

Uutisoinnin ansiosta tietoisuus kyberturvallisuusuhkista ja niiden vakavuudesta on varmasti organisaatioissa kasvanut, mutta haasteena voidaan edelleen pitää sitä, ettei nähdä kyberturvallisuusuhkien yhteyttä organisaation luotettavuuteen ja maineeseen. Tähän osa syy varmasti on siinä, että kyberturvallisuutta käsittelevät artikkelit, kirjallisuus tai uutisointi ovat pitkälti keskittyneet käsittelemään sitä teknisistä, sotilaallisista ja valtiollisista näkökulmista. Vastaavasti maineenhallintaan liittyvät tutkimukset ovat viime vuosina koskeneet sosiaalisen median keskusteluita ja verkkomainontaa. Kyberturvallisuusuhkia, organisaatioiden luotettavuutta ja mainetta yhdistävää tutkimusta ei ole tehty lainkaan.

Näistä syistä tällä tutkimuksella on tarkoitus selvittää:

1. *Miten kyberturvallisuusuhkat liittyvät SaaS-organisaatioiden luotettavuuteen ja maineeseen?*
2. *Miten viestinnällä voidaan vaikuttaa organisaation luotettavuuteen kyberympäristössä?*

Tutkimuksen kohteena ovat SaaS-palveluita tuottavat organisaatiot, joilla liiketoiminta perustuu kokonaan tai lähes kokonaan verkossa tarjottaviin ohjelmistoihin. Tutkimuksessa

keskitytään ulkoisiin sidosryhmiin, koska asiakkaat käyttävät Saas-palveluja vain verkon kautta ja saattavat palvelusta riippuen myös luovuttaa ja tallentaa arkaluontoisia tietoja verkkoon. Näin ollen SaaS-palveluihin käyttöön liittyy olennaisesti luotettavuus ja kyberturvallisuus ja maine.

Tällä tutkimuksella on tarkoitus antaa uutta tietoa siitä, kuinka todennäköisenä kyberturvallisuusuhkia pidetään, miten ne on huomioitu organisaatioiden viestinnässä, ja miten luotettavuutta rakennetaan kyberympäristössä. Viestinnän ammattilaiset voivat saada tämän tutkimuksen avulla lisätietoa kyberturvallisuusuhkista ja organisaatioiden johdolle sekä järjestelmäasiantuntijoille tutkimus voi puolestaan antaa uutta tietoa siitä, etteivät kyberturvallisuusuhkat ole vain taloudellisia ja tietojärjestelmäasioita vaan ne liittyvät myös viestintään, luotettavuuteen ja maineeseen.

1.2 Tutkimuksen rakenne

Tämä tutkimus koostuu johdannon jälkeen seuraavaksi esiteltävästä teoreettisesta taustasta, jossa esitellään tutkimuksen kannalta merkittävimpiä aiempia tutkimuksia sekä käydään läpi keskeiset käsitteet. Kappaleessa 2.7. Organisaatioviestintä kyberympäristössä käsitellään, mitä organisaation viestintä on kyberympäristössä, jonka jälkeen kappaleessa 2.8. käsitellään toimijaverkkoteoriaa. Tutkimuksen toteutus –kappaleessa kerrotaan, tutkimuksesta, joka tehtiin kvalitatiivisena eli laadullisena haastattelututkimuksena kahdeksassa SaaS-organisaatioissa. Lisäksi siinä kerrotaan tarkemmin tutkimuksen rajauksesta, aineiston keruumenetelmästä ja sen analysoinnista. Sen jälkeen kappaleessa 4. Tulokset, tarkastellaan tutkimuksen tuloksia tutkimuskysymysten ja haastattelurungon pohjalta. Johtopäätöksissä tutkimustulokset liitetään teoriaan ja aiempiin tutkimuksiin ja pohditaan tutkimuksen onnistumista sekä mietitään jatkotutkimusaiheita. Viimeisessä kappaleessa annetaan käytännön suosituksia, kuinka SaaS-organisaatioissa voidaan parantaa digitaalista luotettavuutta ja miten kyberturvallisuusuhkat tulisi huomioida organisaatioiden viestinnässä.

2 TEOREETTINEN TAUSTA

Osassa kyberturvallisuutta käsittelevässä kirjallisuudessa viestinnällä nähdään olevan yhteys kyberturvallisuuteen ja -uhkiin. Esimerkiksi kyberturvallisuusuhkat nähdään organisaation sisäisen viestinnän asiana, kuten VTT:n kyberhyökkäyksiä käsittelevässä raportissa. Siinä tuodaan esille, kuinka kyberturvallisuusuhkia voidaan mm. eliminoida, jos organisaation henkilöstö tunnistaa omaa organisaatiota koskevat riskit ja niiden todennäköisyyden toteutua (VTT 2017, 13). Käytännössä tämä tarkoittaa toimivaa sisäistä viestintää. VTT:n raportin tavoin myös Kendrick (2010) pitää kyberturvallisuusriskiviestintää organisaation sisäisenä asiana. Viestintä nähdään tärkeänä osana kyberturvallisuusriskeihin liittyvän strategian jalkauttamisessa henkilökunnalle (Kendrick 2010, 126).

Osa on puolestaan sitä mieltä, että kyberturvallisuusuhkat ovat sekä organisaation sisäinen, että ulkoinen asia. Esimerkiksi Limnéll ym. (2014) näkevät kyberturvallisuuden ja viestinnän Kendrikin tavoin osana organisaation strategiaa eli organisaation sisäisenä asiana, mutta sen lisäksi heidän mielestä kyberturvallisuus ja viestintä koskettavat organisaation kaikkia sidosryhmiä. Kyberturvallisuus tulisi olla mukana kaikessa yrityksen toiminnassa alusta alkaen, ja viestinnän tulisi olla läpinäkyvää. (Limnéll ym. 2014, 14, 24, 56-57, 74.) Luottamus on keskeinen osa kyberturvallisuutta ja siten luottamuksen rakentaminen on tärkein ase kyberturvallisuusuhkia vastaan, ja samalla myös paras perusta kyberturvallisuuden luomiselle (Limnéll ym. 2014, 24-25).

Nurse, Creese, Goldsmith ja Lamberts (2011) ovat keskittyneet kyberturvallisuusviesteihin (risk information, risk message). He luokittelevat kyberturvallisuusriskiviestien luotettavuuteen vaikuttavat tekijät kolmeen pääkategoriaan: lähteeseen/lähettäjään, viestiin/tietoon ja vastaanottajaan. Heidän tutkimus osoitti, että kyberturvallisuusriskejä käsittelevien viestien tulisi olla; hyvin suunniteltuja, yksinkertaisia ja etukäteen vastaanottajilla testattuja. (Nurse ym. 2011, 61, 65-66.) Luotettavuus koskee artikkelissa vain yksittäisiä viestejä, mutta silti nämä kolme tekijää (lähettäjä, viestin sisältö ja vastaanottaja) voidaan katsoa olevan merkittäviä tekijöitä myös organisaatiotason viestinnässä.

Muissa tutkimuksissa on keskitytty enemmän viestin lähettäjän luotettavuuteen ja se on yhdistetty myös kyberturvallisuuteen. Kyberturvallisuusuhkien onnistumisessa on todettu olevan merkitystä viestin lähettäjän luotettavuudella. Positiivinen ennakkoasenne lähettäjästä on yksi vaikuttavista tekijöistä tietojenkalastelun onnistumiseen eli viestin lähettäjän luotettavuus parantaa tietojenkalastelun onnistumista (Pfleeger ja Caputo 2012, 606.)

Viestin lähettäjän luotettavuutta on tutkittu myös aiemmin. Aivan kuten Nurse ym. (2011), jo 50- luvun alussa Howland ja Weis (1951) tulivat siihen tulokseen, että viestijän luotettavuudella on voimakas merkitys. Vaikutus oli suuri heti viestintätilanteen jälkeen, mutta viestijän luotettavuuden merkitys kuitenkin hävisi, kun viestin vastaanottamisesta oli kulunut aikaa. Eli jälkeenpäin muistetaan paremmin viestin sisältö kuin lähettäjä ja hänen luotettavuus. (Howland ja Weis 1951, 647-650.) Myöhemmin Miller ja Baseheart (1969, 6) kuitenkin tulivat siihen tulokseen, että mitä luotettavampi ja uskottavampi viestijä on, sitä tehokkaampaa viestintä on. Vastaavasti 80- luvulla McGinniesin ja Wardin (1980) osoittivat luotettavuuden ja vakuuttavuuden yhteyden. He totesivat, että luotettavuudella oli positiivinen seuraus vakuuttavuuteen, jopa pelkkä lähteen luotettavuus ilman asiantuntijuutta riitti olemaan vakuuttava (Ohanian 1990, 41).

Luottamusta on tutkittu paljon, mutta Mezgár (2006, 454) käsittelee sitä verkkoympäristössä. Hän (Mezgár 2006, 454) esittää, että verkossa viestintätapa ja kesto vaikuttavat luottamuksen tasoon. Hänen mukaan verkossa syntyvissä lyhytaikaisissa suhteissa tulisi luottamus saada rakennettua mahdollisimman nopeasti. Haasteen luottamuksen rakentamiseen ja myös sen ylläpitämiseen verkossa tuo kasvokkaisviestinnän puuttuminen. Ensin luottamus perustuukin vain aavistukseen siitä, että joku on luottamuksen arvoinen, mutta jatkossa kokemukset muokkaavat mielipidettä (Mezgár 2006, 454.)

Kuten huomataan, luottamus ja luotettavuus ovat keskeisiä niin viestinnässä kuin kyberturvallisuudessakin ja lisäksi ne liittyvät maineenhallintaan. Erään tutkimuksen perusteella yrityksen maine koostuu sidosryhmien käsityksistä, odotuksista, kokemuksista ja tunteista (mm. luottamuksesta) organisaation toimintaa kohtaan nyt ja tulevaisuudessa. Vastaavasti sidosryhmien luottamukseen vaikuttaa tutkimuksen mukaan erityisesti mm. organisaation viestintä. (Macmillan, Money, Downing ja Hillenbrand 2005, 220-221; 228-229.)

Maineessa ei kuitenkaan kyse vain luotettavuudesta ja luottamuksesta. Salla-Maaria Laaksonen (2014, 33) on tutkimuksessaan huomannut, että viestien sävyllä on vaikutus organisaation maineeseen. Viestinnän tulee olla johdonmukaista ja linjassa kaiken organisaation toiminnan kanssa, jotta vastaanottajalle ei synny ristiriitaa. Mitä johdonmukaisempaa viestintä on, sitä paremmasta maineesta organisaatio nauttii. (Laaksonen 2014, 33-34). Usein tietojenkalasteluviestien tunnistamiseen liittyen neuvotaan olemaan tarkkana, ovatko viestissä olevat organisaation yhteystiedot, logot, kieli ja viestin sisältö organisaatiolle tavanomaista ja lähetetäänkö viesti vastaanottajalle menetelmällä, jota organisaatio on käyttänyt aiemmin.

SaaS-palveluita ja kyberturvallisuusuhkia yhdistävässä tutkimuksessa korostuu yhteistyö, joka on myös Limnéllin ym. (2014, 83) mielestä yksi tärkeä osa kyberturvallisuusuhkia vastaan koskevassa maineenhallinnassa. Aljawarnehin (2017) tutkimuksen tulos oli, että SaaS-palveluita tarjoavissa organisaatioissa kyberturvallisuusuhkia pidettiin lähinnä väistämättöminä tapahtuvina asioina, jonka johdosta organisaatioissa tulisi tehdä yhteistyötä asiakkaiden ja suunnittelijoiden kanssa, jotta voitaisiin puolustautua kyberturvallisuusuhkia vastaan (Aljawarneh 2017, 385).

Yhteistyön tärkeys kyberturvallisuuden suhteen tulee Aljawarnehin (2017) ja Limnéll ym. (2014) tavoin esille myös Salmanin, Miss Laihan, Babakin, Muzammilin, Sulemanin, Muhammad Khurramin ja Kim-Kwangin (2016) tutkimuksessa. Heidän mukaan kaikkien SaaS-palveluverkoston käyttäjien tulisi huolehtia yhdessä, että viestintä verkostossa on turvallista (Salman ym. 2016, 108).

He ovat myös käsitelleet SaaS-organisaatioille todennäköisimpiä kyberturvallisuusuhkia ja esimerkkeinä mainitaan mm. haittaa tekevät koodit palvelun verkkosivulle, palvelimien kuormituksen ja palveluorganisaation henkilöstön toiminta. SaaS-palveluita koskeva turvallisuus tarkoittaa mm., että asiakkaan tiedot ovat turvassa monenlaisten teknisten toimintojen ansiosta ja että organisaation toiminta on pitkäjänteistä. Turvallisuuden ei kuitenkaan tulisi vaikeuttaa käytettävyyttä tai sitä, ettei käyttäjällä olisi pääsyä palveluihin, joita tarvitsee. (Salman ym. (2016, 103, 105, 115.)

SaaS-organisaatioiden viestintään liittyvää tutkimustakin löytyy, mutta vähän. Öksus (2014) on mm. tutkinut pilvipalveluiden, turvallisuuden, luottamuksen ja viestinnän yhteyttä. Hän on sitä mieltä, että verkkopalveluita käyttäville on viestittävä kyberturvallisuudesta ja se on tehtävä ymmärrettävästi, sillä vastaanottajalähtöisellä hyödyllisellä viestinnällä on vaikutus organisaatiota kohtaan tuntemaan luottamukseen. (Öksus, 2014, 1, 9.) Tyrväinen ja Selin (2011) ovat vastaavasti omassa tutkimuksessaan todenneet, että internet on yksi tärkeimmistä markkinointiviestinnän kanavista SaaS-organisaatioille, mutta myös suosittelijoilla on suuri merkitys. (Tyrväinen ja Selin 2011, 6, 9.)

Kuten nähdään, SaaS-organisaatioilla, kyberturvallisuusuhkilla, viestinnällä, luotettavuudella ja maineella on paljon yhteistä. Ensinnäkin kybertuvallisuusuhkat nähdään SaaS-organisaatioille väistämättömänä ja toiseksi niiden liiketoiminta ja viestintä painottuvat digitaaliseen ympäristöön, johon liittyvät myös kyberturvallisuusuhkat. Vastaavasti kyberturvallisuusuhkiin ja -turvallisuuteen sekä organisaation maineenhallintaan liittyy erottamattomasti viestintä ja sen sisältö, mutta myös vuorovaikutus ja yhteistyö organisaation ja sen sidosryhmien välillä. Lisäksi luottamus on yksi tärkeä tekijä kyberturvallisuudessa, sidosryhmäsuhteissa ja SaaS-organisaatioiden palveluiden käytössä.

2.1 SaaS

Mutta mitä tarkoittaa jo moneen kertaan mainittu SaaS? SaaS on lyhenne sanoista Software-as-a-Service eli se on "*ohjelmisto, jota käytetään vain internetissä ja se on yksi muoto pilvipalveluista*." (Ojala 2013, 1.) Perinteisten ohjelmiston sijasta SaaS-ohjelmistoa ei asenneta organisaation palvelimelle (Tyrväinen ja Selin 2011, 1) ja ohjelmiston käytössä käytettävät tiedot tallennetaan joko julkisiin, yksityisiin tai hybridipilviin. (Ojala 2013, 1.)

Kuten kaikkiin muihinkin asioihin, myös SaaS-palvelun käyttöön liittyy riskejä. Ensinnäkin palvelua käytetään internetverkossa ja toiseksi palvelua käyttävä ei välttämättä tiedä, mihin palvelussa käytettyjä tietoja tallennetaan (Ojala 2013, 3). Turvallisuus onkin yksi merkittävimmistä asioista SaaS-palveluille. Salman ym. (2016) on määritellyt, että SaaS-palveluita koskeva turvallisuus tarkoittaa mm., että asiakkaan tiedot ovat turvassa monenlaisten teknisten toimintojen ansiosta ja että organisaation toiminta on pitkäjänteistä. (Salman ym. 2016, 103, 105, 115.) Siitä huolimatta myös SaaS-palveluverkoston käyttäjien tulisi huolehtia yhdessä, että viestintä on verkostossa turvallista (Salman ym. 2016, 108).

Riskien lisäksi SaaS-palveluilla on paljon etuja, joiden ansiosta palvelut ovat suosittuja. SaaS-palveluiden etuna pidetään ohjelmiston ostamiseen verrattuna mm sitä, ettei se mm. verkossa olevana ohjelmistona vie tilaa organisaatioiden omilta palvelimilta, eikä se vaadi ostavalta organisaatiolta päivityksiä eikä myöskään suuria investointeja (Ojala 2013, 1). Silti asiakkaalla on täydet oikeudet (järjestelmäoikeudet) palveluun (Waters 2005, 33). Palvelua

voikin pitää myös ns. avaimet käteen -palveluna, koska se on asiakkaan käytössä kuukausimaksu- tai lisenssimaksuperiaatteella tai käytön mukaan laskutettavana palveluna. Asiakkaan ei tarvitse huolehtia esimerkiksi päivityksistä tai muusta ylläpidosta, jota ostetun ohjelmiston kohdalla on hoidettava. Koska palvelu on kustannuksiltaan kevyt ja kustannukset ovat ennakoitavissa, SaaS-palvelua käyttävien asiakkaiden koko voi vaihdella pienistä organisaatoista isoihin (Ojala 2013, 1, 3.) SaaS-palveluiden käyttö on myös kasvanut vuosi vuodelta ja niillä on kaikista pilvipalveluista 68,7% markkinaosuus. Vuonna 2017 SaaS-palveluiden määrä kasvoi 22,9% vuodessa (IDC 2017).

Kansainvälinen tietojenhallinnan ammattijärjestö ISACA pitää SaaS-palveluja tarjoavan organisaation mainetta, historiaa ja pysyvyyttä tärkeinä tekijöinä. Myös organisaation kulttuurilla ja toimintavoilla on merkitystä (ISACA 2009, 7). ISACA on listannut - vaikkakin tietoteknisestä näkökulmasta - tekijöitä, jotka ostavan asiakkaan tulisi ottaa huomioon, kun valitsee palvelua tarjoavaa organisaatioita. Nämä viisi tekijää ovat läpinäkyvyys, yksityisyys, lakien ja sääntöjen noudattaminen, vapaasti kulkeva tieto ja sertifiointi. Ymmärrettävästi järjestö keskittyy näihin tekijöihin ohjelmistolähtöisesti. Esimerkiksi läpinäkyvyys, joka viestinnässä tarkoittaa avoimuutta, tarkoittaa tässä yhteydessä tietojen turvassa olemista, ja toisaalta viestintäkanavilla tarkoitetaan sitä, miten ohjelmistossa käytettävät tiedot ja raportit kulkevat suojatusti ulkopuolisilta turvassa. (ISACA 2009, 9.) Mutta nämä kaikki viisi tekijää ovat myös asioita, jotka tulisi viestiä sidosryhmille. Kuten ISACA tuo esille, asiakkaan tulisi olla tietoinen, että SaaS-palveluita tarjoava yritys mm. pitää asiakkaan tiedot turvassa, organisaatio noudattaa lakeja, normeja ja sääntöjä, sillä on alalle tärkeät sertifikaatit kunnossa ja niitä auditoi ulkopuolinen riippumaton taho (ISACA 2009, 9). Näillä tekijöillä voidaan myös olevan vaikutusta organisaation maineeseen, johon on mahdollisuus vaikuttaa organisaatioviestinnällä.

Tässä tutkimuksessa SaaS tarkoittaa ohjelmiston tarjoamista verkkopalveluna ja SaaS-palveluita tarjoavana organisaationa pidetään puolestaan yritystä, joka tarjoaa SaaS-palveluita internetin välityksellä kuukausi- tai muuta vastaavaa korvausta vastaan.

SaaS-organisaatioiden toimintaympäristöstä johtuen niiden organisaatioviestinnässä voidaan pitää tärkeänä digitaalista, verkossa tapahtuvaa viestintää, jonka tulisi olla avointa, tuoden esille organisaation historiaa, SaaS-palvelun turvallisuutta, luottamuksellisuutta ja alaan liittyvien sertifikaattien noudattamista.

2.2 Kyberympäristö ja -turvallisuus

Kyberympäristön määritelmissä on paljon yhtenäistä. Kaikissa tuodaan esille laitteet ja viestintä. Suomen tietoliikenteen ja tietotekniikan keskusliiton (FiComin) kyberympäristön määritelmässä tulee näiden lisäksi esille ympäristön verkostomaisuus: ”*Kyberympäristö muodostuu yhdestä tai useasta tietojärjestelmästä*” (FiCom, 1). Se myös sisältää fyysiset puitteet ja systeemit, joissa tietoa käsitellään (FiCom 1). Hyvin samankaltainen määritelmä on Suomen kyberturvallisuusstrategiassa (2013, 12, 17), jossa kyberturvallisuusympäristöä pidetään digitaalisena ja sähköisenä toimintaympäristönä, johon niin ikään liittyvät tietojärjestelmät ja tiedon käsittely. Strategiassa kuitenkin lisätään määritelmään myös kyberympäristön reaaliaikaisuus, jossa ollaan enemmän yhteydessä toisiin (Suomen kyberturvallisuusstrategia 2013, 12, 17).

Juhani Latvakosken (2016) kyber-fyysisen järjestelmän (cyber-physical system, CPS) käsite sisältää edellisten määritelmien lisäksi vuorovaikutuksen aspektin ja luotettavuuden. Hänen mielestään kyber-fyysinen järjestelmä on ihmisten, laitteiden ja koneiden luoma yhteinen ympäristö, jossa ne voivat olla yhteydessä toisiinsa langattomasti ja vaihtaa tietoa keskenään luotettavasti. (Latvakoski 2016, 19).

Latvakosken (2016) tavoin Limnéllin ym. (2014) mukaan kybermaailmassa tapahtuu vuorovaikutusta, johon meidän fyysinen maailma on sekoittunut. Mutta muista määritelmistä poiketen, he tuovat esille, että lähes kaikissa fyysisen maailman toiminnoissa on tultu riippuvaisiksi digitaalisesta maailmasta, esimerkiksi älypuhelimet, kodin lämmitysjärjestelmät tai sydämentahdistimet ovat osa niin fyysistä kuin kyberympäristöäkin (Limnéll ym. 2014, 29, 31-32). Silloin puhutaan esineiden internetistä (Internet of Things, IoT), jossa laitteita ja koneita hallitaan verkon kautta (Lönnqvist ja Moilanen 2017, 8).

Tämän työn kannalta paras yksittäinen selitys kyberympäristölle on Dasguptan (2006, 4) määritelmä:

" *Cyberspace is the total interconnectedness of human beings trough computers and telecommunication without regarded to their geographical location*."

Tässä määritelmässä kyberympäristö ei ole paikkaan sidottu, ja siellä yhdistyvät tietokoneet viestintä ja ihmiset. Nykyään kyberympäristön määritelmään tulee lisätä myös esineiden internet, koska myös muut kuin tietokoneet ja ihmiset ovat yhteydessä toisiinsa. Lisäksi tässä tutkimuksessa kyberympäristöä pidetään kybermaailmana, joka on keinotekoinen ihmisen luoma maailma, jossa vuorovaikutus on reaaliaikaista ja se on osa jokapäiväistä elämää, jota ilman emme voisi enää olla.

Tutkimuksen haastatteluissa päädyttiin käyttämään kyberympäristön sijasta käsitettä digitaalinen ympäristö, koska sen oletettiin olevan haastateltaville ymmärrettävämpi mitä kyberympäristö. Näitä kahta käsitettä voidaan pitää lähes toistensa synonyymeinä. Syuntyurenko (2015, 24) on esimerkiksi määritellyt digitaalisen ympäristön rakentuvan ensisijaisesti internetistä, johon sisältyy sosiaaliset verkostot, mobiilisovellukset (älypuhelimet ja tabletit) ja maksujärjestelmät. Internetin lisäksi digitaalinen ympäristö koostuu myös esineiden internetistä (Internet of Things, IOT) ja ns. BodyNetistä eli mikrosiruista, joita voi vaatteissa ja laitteissa, esimerkiksi sydämentahdistimessa, joka sirun kautta voidaan yhdistää digitaaliseen ympäristöön. Kuten huomataan, on digitaalisen ympäristön määritelmä hyvin pitkälle sama kuin kyberympäristön. Kummassakin määritelmässä vuorovaikutus ei ole paikkaan sidottua, se koostuu ihmisistä ja laitteista ja heidän välisestä vuorovaikutuksesta ja molempia kuvastaa keinotekoisuus, reaaliaikaisuus ja välttämättömyys osa arkea. Tästä syystä digitaalisen ympäristö -käsitteen käyttäminen haastatteluissa katsottiin perustelluksi.

Kyberturvallisuus on vastaavasti osa kyberympäristöä. Kaikissa löydetyissä määritelmissä nousee sen lisäksi esille, että se on sekä saavutettu tavoite, mutta myös joukko toimenpiteitä. Brookson, Cadzow, Eckmaier, Eschweiler, Gerber, Guarino, Rannenberg, Shamah ja Górniak (2016) ovat todenneet, että kyberturvallisuuden määritteleminen vain yhdellä tapaa on haasteellista ja jopa mahdotonta, mutta joka toisaalta turvallisuuden nimissä tulisi saada tehtyä. Esteitä määritelmän standardoimiselle tuo mm. kyberympäristön nopea muuttuminen, eri toimialojen erilaiset ja toisistaan poikkeavat uhkat sekä eri järjestelmien ja algoritmien käyttö. Lisäksi haasteena on, että standardointia tehdään niin kansainvälisellä, kansallisella että toimialatasolla, ja ne eivät vastaa toisiaan (Brookson ym. 2016, 24, 26-27).

Tähän tutkimukseen sopii hyvin Kansainvälisen televiestintäliiton (ITUn) alaisuudessa toimivan televiestinnän standardoimistoimisalan (ITU-T:n) määritelmä kyberturvallisuudelle, johon liittyy myös sidosryhmäviestintä. Sen mukaan kyberturvallisuus kattaa erilaisia toimenpiteitä mm. riskienhallintaa, toimia, koulutusta, ohjeita ja parhaita toimintatapoja, joiden tarkoituksena on turvata ja suojata verkkoympäristö organisaation ja sen sidosryhmien välillä ja kesken. Kyberturvallisuus sisältää laitteiden lisäksi henkilöstön, infrastruktuurin, sovellukset, järjestelmät, lähetetyt tiedot ja tiedot verkossa - kaiken, joka liittyy kyberympäristöön ja sitä kuvastaa luottamuksellisuus ja aitous. (ITU-T 2008, 2.)

FiComin määritelmässä kyberturvallisuus nähdään tilana, jota tavoitellaan, mutta toisaalta se nähdään joukkona keinoja, joilla ennalta varaudutaan uhkiin. Keinojen tarkoitus on myös ”*…hallita ja tarvittaessa sietää erilaisia kyberuhkia*” (FiCom, 1). Toimenpiteet tulevat esille myös Lehdolla ja Neittaanmäellä (2014), joiden mukaan kyberturvallisuus on joukko toimenpiteitä, joilla pyritään tekemään tietojärjestelmistä parempia, torjutaan riskejä ja korjataan heikkouksia. He myös määrittelevät kyberturvallisuuden perustuvan organisaation arvioon tai aavistukseen uhkista (Lehto ja Neittaanmäki 2014, 25).

Näiden määritelmien lisäksi kyberturvallisuus nähdään kenttänä, joka tulee horjuttamaan turvallisuuden tunnetta uudella tavalla: ”*Kyberturvallisuus on turvallisuuden alue, joka muuttaa mitä keskeisimmin ymmärrystämme turvallisuudesta lähivuosien aikana*.” ja ettei ”*…täydellistä kyberturvallisuutta ole olemassa*” (Limnéll ym. 2014, 15-16).

Viestinnän kannalta kyberturvallisuuden määritelmässä on olennaista, ettei kyberturvallisuuden tila ole pysyvä eikä absoluuttinen ja, että yhtä varmaa on sen epävarmuus. Voidaankin sanoa, että kyberturvallisuusviestinnän tulisi olla proaktiivista ja kyberturvallisuus tulisi huomioida niin sisäisessä kuin ulkoisessakin viestinnässä, ja tiedottamisen lisäksi tulisi olla kouluttamista ja yhteistyötä. Tärkeänä voidaan nähdä myös yhteisten käytänteiden ja vuorovaikutuksen jatkuvaa ylläpitämistä muiden sidosryhmien kanssa. Kyberturvallisuutta koskeva viestintä liittyy myös riski- ja kriisiviestintään, jolloin luodaan valmiuksia kyberturvallisuusuhkien aiheuttamien kriisien ennaltaehkäisemiseen ja niiden toteutuessa nopeaan tilanteen palauttamiseen.

2.3 Kyberturvallisuusuhkat – ja riskit

Kuten kyberturvallisuuden määritelmistä kävi ilmi, liittyvät kyberturvallisuusuhkat ja -riskit kiinteästi kyberturvallisuuteen, mutta myös toisiinsa. Kummankaan määrittely ei ole kuitenkaan helppoa, sillä osassa kirjallisuutta kyberturvallisuusuhkaa ja -riskiä pidetään toistensa synonyymeinä. Varsinkin englanninkielessä sekä uhka että riski ilmaistaan joskus pelkästään sanalla ”risk” ja myös eri tieteenalat ja tutkimukset käyttävät käsitteitä eri tavalla. Tässä tutkimuksessa käsitteet kyberturvallisuusuhka ja -riski tarkoittavat eri asioita.

Taulukkoon 1 on koottu määritelmiä kyberturvallisuusuhkalle. Olennaista on, että kyberturvallisuusuhkat liittyvät kyberympäristöön (Suomen turvallisuusstrategia 2013, 13, 18 ja ENISA 2017, 30) ja tietojärjestelmiin (Oxford sanakirja). Ne ovat ensisijaisesti kohdistettu digitaaliseen maailmaan ja siihen yhteydessä oleviin laitteisiin (Oxford sanakirja, Limnéll ym. 2014, 23, 106-107). Kyberturvallisuusuhkat koskettavat lopulta myös fyysistä ympäristöä ja ihmisiä (Suomen kyberturvallisuusstrategia 2013, 12) ja ne voivat olla vahingossa tai

tahallaan tehtyjä (Limnéll ym. 2014, 37) tai välillisiä tai suoraan tehtyjä (Suomen kyberturvallisuusstrategia 2013, 18). Merkittävää on myös, että tekijä voi olla tuttu tai tuntematon (Limnéll ym. 2014, 23, 37, 106-107) ja kyberturvallisuusuhkiin liittyy taloudellinen tai maineriski (World Economic Forum 2015, 5).

TAULUKKO 1. Määritelmiä kyberturvallisuusuhka käsitteelle.

Kyberturvallisuusuhka
Kyberturvallisuusuhka on mahdollisuus toimenpide tai tapahtuma, joka uhkaa kyberympäristöstä riippuvaa toimintaa. ”Kyberuhkamallissa kyberuhkia ovat: kyberaktivismi (kybervandalismi, haktivismi), kyberrikollisuus, kybervakoilu, kyberterrorismi ja kyberoperaatiot; painostus, sotaa alempi konflikti tai sotaan liittyvä kyberoperaatio.” Suomen kyberturvallisuusstrategia. (2013, 12-13, 18).
Kyberturvallisuusuhka on vahinko tai tahallaan toteutettava, jossa voivat yhdistyä fyysisen ja digitaalisen ympäristön keinot. Se voi tulla organisaation sisältä tai ulkoa ja sillä olla vaikutus maineeseen ja talouteen. Pääasiassa tekijöinä ovat työntekijät, tai organisaation muut sidosryhmät, jotka kokevat tyytymättömyyttä. Limnéll, Majewski ja Salminen (2014, 23, 37, 106-107)
Kyberturvallisuusuhka (threat) on aikomus toimenpiteistä, jotka kohdistuvat tietojärjestelmiin, ja joilla on tarkoitus päästä käsiksi luvatta ja ilmoittamatta toisten tietoihin tai väärentää toisten identiteettejä sekä tehdä palvelunestohyökkäyksiä (Oxford sanakirjamääritelmä)
Kyberturvallisuusuhkat ovat asioita, joista haavoittuvuuksien johdosta muodostuu joko taloudellisia tai maineriskejä (World Economic Forum 2015, 5).
Kyberturvallisuusuhkia ovat esimerkiksi kyberympäristössä tapahtuvat väärennökset, varkaudet ja petokset (ENISA, 2017, 30).

Suomen kyberturvallisuusstrategiassa (2013, 18) kyberturvallisuusuhkia on luokiteltu viiteen eri kategoriaan. Kyberaktivismi käsittää verkossa tapahtuvan haktivismin, jossa yleensä toimintapa on palvelunestohyökkäys eli organisaation sivustoille luodaan niin paljon liikennettä, että sivustot kaatuvat. Haktivistimiin liittyy myös asiakastietojen ja kävijätietojen varastaminen (Peltomäki ja Norppa 2015, 46.). Kyberrikollisuuden tarkoitus on haitan sijaan rahallisen hyödyn tavoittelu (Peltomäki ja Norppa 2015, 45-48), esimerkiksi väärennökset, varkaudet ja petokset (Enisa 2017, 30). Kybervakoilun Lehto ja Neittaanmäki (2015, 12) määrittelevät toiminnaksi, joissa tarkoituksena on saada salassa pidettävää, yksityistä tietoa, yksityisiltä ihmisiltä, organisaatioilta ja vastaavilta, hyödyntäen verkkoa ja siihen liittyviä laitteita laittomin keinoin poliittisiin, taloudellisiin tai sotilaallisiin tarkoituksiin. Peltomäen ja Norpan (2015, 48) mukaan kybervakoilu voidaan jakaa teollisuus- ja talousvakoiluun, joista teollisuusvakoilua on mm. tuotekehitystietojen anastaminen verkon välityksellä. Edellä mainitut uhkat voivat tulla organisaation ulkoa tai sisältä (Limnéll ym. 2014, 37, Kramer ja Cook 2004, 11).

Kyberturvallisuusriskeille löytyy myös useita eri määritelmiä. Kendrickin (2010, 86) mukaan kyberturvallisuusriskien määrä on niin suuri, ettei niistä voi tehdä yhtä ainoaa oikeaa luetteloa, koska jokin riski toiselle ei ole sitä välttämättä toiselle. Tätä näkemystä tukee myös uudempi Elingin ja Schnellin (2016, 476) tutkimus, jota varten he löysivät 209 erilaista kyberturvallisuusriskin määritelmää. Tähän tutkimukseen parhaiten sopivat kyberturvallisuusriskin määritelmät on koottu taulukkoon 2.

TAULUKKO 2. Määritelmiä kyberturvallisuusriskille.

Kyberturvallisuusriski
Kyberturvallisuusriski on tahallinen tai tahaton, joiden toteutustapa ja tekijä voivat vaihdella ja syynä voi ihmisen lisäksi olla luonnonkatastrofi (Eling ja Schnell 2016, 17 ja 2015,12).
Kyberturvallisuusriski on mm. toimintaan liittyvä riski ja se on organisaatiolähtöinen. Se johtuu organisaation strategioista, osaamisesta, käytänteistä, toimintatavoista ja suhteista asiakkaisiin ja henkilöstön johtamisesta (Kendrick 2010, 25.)
Kyberturvallisuusriski on tietojärjestelmien haavoittuvuudesta ja ongelmista johtuva mahdollisuus, jossa organisaation maine kärsii ja organisaatio kokee taloudellisia menetyksiä (IRM 2018).
Kyberturvallisuusriski on vahingontekomahdollisuus, joka kohdistuu kyberympäristöön ja toteutuessaan aikaansaa ongelmia ja häiriöitä (Suomen kyberturvallisuusstrategia 2013, 12).
Kyberturvallisuusriski on seuraus aiemmin sattuneesta asiasta, joihin voidaan varautua riskienhallinnalla. Uhkien sijaan riskeihin voidaan vaikuttaa (Limnéll ym. 2014, 108).
Kyberturvallisuusriski on potentiaalinen negatiivinen teko, josta voi seurauksena olla kriisi, jos uhkana on organisaation toimintakyky ja luottamus (Lehtonen 2009, 9).

Kuten nähdään, Elingin ja Schnellin tutkimuksessa (2016) kyberturvallisuusriskit on jaettu rikollisuuden, luonteen ja tekijän mukaan. Rikolliset riskit voivat olla mm. kiristys, petos, rikollisuus, sota tai terrorismi tai riskejä ilman rikosta esim. vahinko. Riskien luonteen tarkastelu tarkoittaa mm. sitä, ovatko ne esim. roskaposteja, organisaation sisältä tulevia iskuja vai haittaohjelmia. Tekijän jaottelussa tarkastellaan, onko tekijä esim. yksittäinen henkilö, terroristi, rikollinen vai hallitus (Eling ja Schnell 2016, 17) tai onko kyberturvallisuusriskin aiheuttaja luonnonkatastrofi esim. tulva tai maanjäristys (Elling ja Schnell 2015, 12).

Osa kyberturvallisuusriskien määritelmistä käsittää organisaation toiminnan. Kendrick (2010) jaottelee kyberturvallisuusriskit teknologia-, lainsäädäntö- ja toimintariskeihin, joista tämän työn kannalta merkittävimpinä voidaan pitää organisaation toimintaan liittyviä kyberturvallisuusriskejä. Niissä kyse on sidosryhmäsuhteista, johtamisesta ja organisaation käytänteistä. (Kendrick 2010, 24-25, 37.) Organisaation toiminta on mukana myös Limnéllin ym. (2014) määritelmässä, jonka mukaan kyberturvallisuusriski on seuraus aiemmin sattuneesta asiasta eli toiminnasta.

Riskienjohtamisen instituutin (IRM 2018) ja Lehtosen (2009, 9) määritelmissä esille nousee muista poiketen maine. IRM:n mukaan kyberturvallisuusriski on tietojärjestelmien haavoittuvuudesta ja ongelmista johtuva mahdollisuus, jossa organisaation maine kärsii ja organisaatio kokee taloudellisia menetyksiä. IRM tuo myös esille, että riskit voivat olla organisaatiolle hyvä asia, jos se osaa hallita niitä. Riskienhallinta on mm. keino erottua kilpailijoista ja lisätä asiakkaiden luottamusta. (IRM 2018). Lehtonen (2009, 9) on ainoa, jonka määritelmä tuo esille, että riskistä voi seurata kriisi.

Puhutaanko siis kyberturvallisuusuhkista vai kyberturvallisuusriskeistä? Tähän tutkimuksen tehdyn kattavan aineistohaun perusteella voidaan todeta, että käsitteiden välillä on sekä yhteneväisyyksiä että eroavaisuuksia. Jyväskylän yliopiston ohjelmisto- ja tietoliikennetekniikan professorin Timo Hämäläisen mielestä ”eksaktia määritelmää” määritelmien eroavaisuuksista ei ole tehtävissä. Hänen mielestä hyvä keino erottaa käsitteet toisistaan on riskianalyysi, jonka jaottelu on myös Hämäläisen oman tutkimuksen taustalla: ”*Kyberuhkia*

ovat hyökkäykset ja kyberturvallisuusriskejä mahdolliset kohteen (ihmiset, tietojärjestelmät) haavoittuvuudet." (Hämäläinen 2018).

Hämäläisen näkemystä kyberturvallisuusuhkien ja -riskien erosta tukee myös maailman talousfoorumi. Maailman talousfoorumi (World Economic Forum 2015) näkee kyberturvallisuusuhkat (esim. haktivismin ja yritysvakoilun) asioina, joista haavoittuvuuksien (ihmisten, laitteiden ja prosessien aiheuttamien tahattomien vahinkojen ja/tai huonojen toimintojen) johdosta muodostuu, joko taloudellisia tai maineriskejä. Raportista on olennaista tuoda esille, että kyberturvallisuusriskeihin voidaan vaikuttaa mm. yhteisössä ja organisaatioissa tapahtuvalla yhteistyöllä, tietojen jakamisella ja johdetuilla toimilla sekä organisaation toimintaan ja järjestelmiin juurrutetulla kyberturvallisuudella. (World Economic Forum 2015, 5.).

Limnéllin ym. (2014, 108) mukaan uhkan ja riskin ero on siinä, että uhkia voidaan torjua, mutta riskeihin voidaan varautua. Uhka on asia/tila, jossa ei vielä tapahdu vahingontekoa. Tekijästä, kohteesta ja toteutustavan todennäköisyydestä riippuu, kuinka uskottavana uhkan toteutumaa eli riskiä pidetään. He ovat myös sitä mieltä, etteivät kyberturvallisuusuhkat ja -riskit eroa "normaaleista" uhista ja riskeistä muutoin kuin toimintaympäristönsä vuoksi. (Limnéll ym. 2014, 106, 108.)

Tässä työssä kyberturvallisuusuhka ja -riski erotetaan ensisijaisesti Timo Hämäläisen ja maailman talousfoorumin ajatusten mukaisesti, mutta molemmat käsitteet ovat yhdistelmiä useista määritelmistä.

Kyberturvallisuusuhka *on mahdollinen tahaton tai tahallinen teko, joka kohdistuu laitteisiin, järjestelmiin ja ihmisiin, jotka ovat yhteydessä toisiinsa kyberympäristön kautta. Kyberturvallisuusuhka koskettaa täten kyberympäristön lisäksi fyysistä maailmaa, koska lähes kaikki on kytketty kyberympäristöön.*

Kyberturvallisuusriski *on kyberuhkan seuraus. Kyberturvallisuusriski on kohteen haavoittuvuus, joka koskee organisaation järjestelmiä, mainetta, luottamusta, taloutta ja toimintaedellytyksiä. Kohteen haavoittuvuuden lisäksi riskiin vaikuttavat iskun tekijä, hänen taidot ja tekotapa, ennakoitavuus sekä teon laajuus. Kyberturvallisuusriskiin liittyy aina kriisin mahdollisuus, mutta varautumalla riskeihin, esimerkiksi riskianalyysillä, kriisejä ja niiden kestoa sekä laajuutta voidaan vähentää tai eliminoida kokonaan.*

2.4 Luotettavuus

Luotettavuudesta on useita erilaisia määritelmiä ja toisaalta ollaan sitä mieltä, ettei sitä voi määritellä ollenkaan. Taloudellisesta näkökulmasta tarkasteltuna luotettavuudessa on kyse organisaation tulo- ja kustannusjakaumilla ja konkurssiriskillä (Forbes, kansainvälinen talouslehti).

Useissa tutkimuksessa luotettavuus on liitetty uskottavuuteen. Pornpitakpan (2004) on tutkinut lähteen uskottavuutta koskevia tutkimuksia useilta eri vuosikymmeniltä ja

myös hän on tullut tulokseen, että lähestulkoon kaikissa tutkimuksissa luotettavuutta on pidetty yhtenä uskottavuuden osatekijänä. Uskottavuuteen liitetään usein myös asiantuntijuus, mutta Pornpitakpanin (2004) mukaan tutkimukset eivät osoita selkeästi, kumpi on tärkeämpi – luotettavuus vai asiantuntijuus, kun kyse on uskottavuudesta. (Pornpitakpan, 2004, 269.)

Esimerkkinä luotettavuuden ja uskottavuuden välisestä yhteydestä mainittakoon Howlandin ja Weisin (1951) sekä Ohanian (1990) tutkimukset, joissa luotettavuus on yksi tekijä mitattaessa uskottavuutta. Luotettavuus muodostui Ohianin (1990) tutkimuksessaan viidestä tekijästä, joista kolme suomennetaan luotettavuudeksi (dependable, reliable ja trustworthy). Sen lisäksi luottavuuteen liittyivät rehellisyys (honest) ja vilpittömyys (sincere). Tutkimuksen lopputulos oli, että luotettavuus, asiantuntijuus ja vetovoima korreloivat keskenään, eli niillä on vaikutusta toisiinsa ja luotettavuus vaikuttaa lähteen uskottavuuteen. (Ohanian 1990, 39, 46,50.)

Myös Mae Kim ja Brown (2015) ovat tulleet tulokseen, että luotettavuus on osa uskottavuutta. Tutkimuksen mukaan on neljä tapaa, jolla organisaatio voi olla uskottava sosiaalisessa mediassa. Organisaation on oltava miellyttävä, sen on osattava asiansa, eli on oltava oman liiketoimintansa asiantuntija ja. sen on oltava vuorovaikutuksessa eli pelkkä sisällönluominen ei riitä. Verkossa on keskusteltava yleisön kanssa, sitä on myös kuunneltava ja sitä kohtaan on rakennettava ymmärrystä. Neljäs organisaation uskottavuuteen vaikuttava tekijä sosiaalisessa mediassa on luotettavuus. Organisaation on oltava rehellinen ja läpinäkyvä ollakseen luotettava. Luotettavuutta voi vahvistaa mm. tuomalla esille, kuinka se on pitänyt lupauksena ja kuinka se noudattaa säädöksiä ja lakeja. (Mae Kim ja Brown (2015, 1, 10-12.)

Mae Kimin ja Brownin (2016) tavoin myös Gefenin, Benbsatin ja Pavloun (2008, 282) mielestä organisaation tulisi kiinnittää huomiota, miten organisaatio on läsnä ns. kirjallisesti kyberympäristössä. Tekstin avulla organisaatio voi heidän mielestä tuoda esille kykyään, hyväntahtoisuuttaan ja rehellisyyttään. Nämä vaikuttavat kuluttajien luottamuksen syntymiseen ja lopulta mahdolliseen ostopäätökseen. (Gefen, Benbsati ja Pavlou 2008, 282.)

Lisäksi Wiencierz, Pöppel ja Röttger (2015) ovat sitä mieltä, että luotettavuudella ja maineella on yhteys ja, että organisaation toimet, jotka herättävät luottamuksen kokemuksen, voivat vaikuttaa positiivisesti organisaation maineeseen ja toisaalta taas organisaation maine voi ennustaa luotettavuuden kokemusta. (Wiencierz ym. 2015, 103-104, 106, 113.)

Luotettavuuteen liittyvät siten myös kokemukset. Yritysten välisessä toiminnassa merkitystä on lisäksi sillä, mitä organisaatiosta tiedetään muiden kumppaneiden kautta ja toisaalta, mitä suoria kokemuksia organisaatiolla on. Edelleen merkitystä on, miten organisaatio tuo esille luotettavuuttaan. Merkkejä luotettavuudesta osoittavat mm. maine, brändi ja laatuvaatimusten hyväksyminen. Maineella on erityisesti merkitystä silloin, jos oma kokemus organisaatiosta puuttuu. Tuolloin korostuvat muiden kokemukset (Kramer ja Cook 2004, 159.)

Digitalisoitumisen myötä on herännyt myös tarve eritellä luotettavuus ja digitaalinen luotettavuus. Mezgár (2006, 454) määrittelee näiden eron seuraavasti:

> ” *Trustworthiness is the ability to attain and maintain a trusted state, which is definable, measurable, validatable, and demonstrable over time. Digital trustworthiness means a verifiable level of electronic process integrity, security, control, authenticity, and reliable, that captures, preserves, retrieves, verifies, renders, and makes available in human readable form the essential transaction content, context, notice, intent, and consent to meet the electronic forensic evidence requirements necessary for legal admissibility and regulatory compliance.* “

Mezgárille (2006) luotettavuus on luottamuksen saavuttamista ja ylläpitämistä, ja digitaalinen luotettavuus tarkoittaa enemmänkin teknistä luotettavuutta siitä, että verkossa käytävä vuorovaikutus, tietojen antaminen ja jakaminen tapahtuvat luotettavasti sekä turvallisesti. Lisäksi digitaaliseen luotettavuuteen sisältyy tiedon olennaisuus ja oikea muoto vastaanottajalle. Digitaalinen luotettavuus on sekä teknologia- että ihmislähtöistä ja käyttäjän / kuluttajan omassa luottamuksessa yhdistyvät nämä molemmat. Verkkoluotettavuudessa yhdistyy esimerkiksi tieto siitä, säilyvätkö arkaluontoiset tiedot turvassa (teknologialähtöinen luottamus) ja kokemus siitä, kuinka läpinäkyvää viestintä on ja kuinka helppoa verkkosivustoja on käyttää (ihmislähtöinen luottamus) (Mezgár (2006, 454.)

Kun Mezgáril näkee luotettavuuden luottamuksen saavuttamisena ja ylläpitämisenä Lane ja Backhamn (2000, 75) kuvaavat puolestaan luotettavuuden *rakentamista "monimutkaisena, dynaamisena ja jatkuvana prosessina."* Sen lisäksi luotettavuudella *"luodaan merkityksiä muille"* Lane ja Backhamn 2000, 75.) Käytännössä merkitysten luomisena voidaan pitää esimerkiksi lisäarvon tuottamista. Lane ja Backhamn (2000) näkevät, että selvittääkseen organisaation luotettavuuden muodostumisen, tulisi tarkastella vuorovaikutustilanteita, joissa luottamusta voi syntyä. He kuitenkin huomauttavat, etteivät pelkät vuorovaikutustilanteet vaikuta organisaation luotettavuuteen vaan myös organisaation toimialalla, maalla ja verkostoilla, joissa organisaatio toimii, on merkitystä. (Lane ja Backhamn 2000, 47.) Tässä tutkimuksessa käsitellään digitaalista luotettavuutta eli luotettavuutta kyberympäristössä.

Digitaalinen luotettavuus *syntyy kyberympäristössä sen ulkoisissa sidosryhmissä ja vuorovaikutus tapahtuu pääsääntöisesti verkossa. Se syntyy, kun kokemukset organisaatioista ovat positiiviset ja, kun organisaatio pyrkii varmistamaan kaikella toiminnallaan, että tietojen jakaminen ja tallentaminen – ylipäätään vuorovaikutus verkossa on turvallista ja viestintä on asiantuntevaa, avointa, rehellistä, läpinäkyvää ja johdonmukaista sekä sidosryhmälähtöistä. Lisäksi organisaation luotettavuuteen vaikuttavat omat ja muiden kokemukset. Luotettavuus vaikuttaa maineeseen ja toisaalta maine vaikuttaa luotettavuuteen. Luotettavuus ei ole pysyvää vaan sitä kuvastaa jatkuva muutos.*

2.5 Luottamus

Luottamuksen määritelmät ovat jossain määrin samankaltaisia mitä luotettavuuden määritelmät ja joskus niitä jopa pidetään toistensa synonyymeina. Näin ei kuitenkaan ole, sillä käsitteissä on näkökulmaero.

Esimerkiksi Mayer, Davis ja Schoorman (1995, 715) ja myöhemmin Wiencierz, Pöppel ja Röttger (2015) ovat tulleet tutkimuksissa siihen tulokseen, että organisaation luotettavuus on ennen luottamusta. Organisaation luotettavuus on perusta luottamukselle ja luotettavuus syntyy kyvystä, hyväntahtoisuudesta ja rehellisyydestä. Näiden ominaisuuksien olemassaolo kertoo organisaation keinoista selviytyä tulevaisuudessa. (Wiencierz ym. 2015, 103-104, 106, 113.)

Yhteiskunnan muuttuminen teknologiaväitteisemmäksi on tuonut mukanaan tarpeen miettiä luottamuksen käsitettä myös virtuaalimaailmassa. Giustiniano ja Bolici (2012, 187)

ovat sitä mieltä, että luottamus ei ole pysyvää vaan siihen vaikuttavat erilaiset sosiaaliset, taloudelliset ja tekniset olosuhteet. Silti voidaan sanoa, että aina luottamuksessa on kyse kahden osapuolen välisestä vuorovaikutuksesta. Puhutaan toimijasta (trustor) ja vastapuolesta, johon luotetaan (trustee). Toimijan luottamuksen kohde voi olla mikä tahansa, eli myös tekninen laite. (Giustiniano ja Bolici 2012, 187.) Giustiniano ja Bolici (2012, 188) tuovat kuitenkin esille, että luottamus teknologiavälitteisessä ympäristössä määritellään hyvin monella tapaa, eikä sille ole olemassa yhtä selkeää määrittelyä.

Puhuttaessa luottamuksesta tieto- ja viestintäteknologiavälitteisessä (ICT = Information and Communication Technologies) ympäristössä, voidaan luottamus jakaa - luotettavuuden tavoin, sosiaaliseen ja teknologiseen luottamukseen. Sosiaalinen luottamus on ihmisten välistä, joka syntyy kyberympäristössä erilaisissa verkostoissa esimerkiksi intranetissä tai keskusteluryhmässä. Sosiaalinen luottamus vaikuttaa siihen, miten ihmisten käytös muuttuu ja identiteetti paranee (translation). Seurauksena voi olla verkoston toiminnan stabiloituminen. Teknologisella luottamuksella tarkoitetaan vastaavasti ihmisten luottamusta teknologiaa kohtaan. Laitteet voivat vaikuttaa ihmisten rooleihin kyberympäristössä, joten luottamuksella on tärkeä merkitys koko kyberympäristön toiminnan kannalta. Nämä molemmat luottamukset vaikuttavat toisiinsa, kuitenkin niin, että jos ihmisillä ei ole luottamusta teknologiaan, on sillä vaikea luoda myös sosiaalista luottamusta, koska sen luomiseen tapahtuva vuorovaikutus tapahtuu ainoastaan kyberympäristössä. (Giustiniano ja Bolici 2012, 192-194.)

Luottamus liitetään usein myös riskin ottamiseen. *"Luottamus on halua ottaa riski ja luottamuksen taso määrittää, kuinka isoja riskejä on valmis ottamaan."* (Schoorman, Mayer ja Davis 2007, 346). Määritelmä sopii hyvin kyberympäristöön, jossa toimiakseen on väistämättä otettava riskejä.

Luottamuksessa ja myös riskien ottamisessa on kyse tunteista – ainakin osittain. Schoorman, Mayer ja Davis (2007, 348) ovat sitä mieltä, että luottamukseen liittyvät aina tunteet, mutta Kuzheleva-Sagan ja Suchkova (2016, 384) mukaan Sztompka (2012, 76), on luokitellut luottamuksen kolmitasoiseksi, ja on sitä mieltä, että tunteet liittyvät vain kahteen ensimmäiseen tasoon. Ensimmäisellä tasolla luottamus perustuu ulkoisiin tekijöihin, maineeseen ja suosituksiin. Toisella tasolla se perustuu läpinäkyvyyteen, avoimuuteen ja asian yhteyteen. Kolmannella tasolla luottamuksesta on kyse rationaalisesta arvioinnista ja subjektiiviseen tulkintaan saatavilla olevasta informaatiosta. Sztompkan (2012, 82) mielestä nykyajan luottamus tarkoittaa lisäksi epävarmuutta ja sitoutumista tulevaan, koska ei voi tietää tehtyjen asioiden seurauksia (Kuzheleva-Saganin ja Suchkovan 2016, 383 mukaan).

Edellä olevien lisäksi luottamukseen kyberympäristössä vaikuttavat organisaation verkkosivut. Zhu, Lee, O'Neal ja Chen (2011, 12) osoittivat omassa tutkimuksessa, että mm. verkkosivujen helppokäyttöisyydellä oli vaikutusta luottamuksen syntyyn ja vastaavasti luottamuksella oli merkitystä verkkosivujen kautta koettuun hyödyllisyyteen (verkkosivut sisältävät kuluttajalle tärkeää informaatiota). Luottamus, helppokäyttöisyys ja hyödyllisuus vaikuttivat positiivisesti asenteeseen ja lopulta ostopäätökseen. Lisäksi verkkosivuilla vierailujen korkean määrän katsottiin liittyvän korkeampaan luottamukseen organisaatiota kohtaan. (Zhu ym. 2011, 13.)

Verkkokauppaa koskevassa tutkimuksessa (Castelfranchi ja Tan 2002, 55), on todettu luottamuksen vaikuttavan myös ostokäyttäytymiseen, jonka johdosta luottamuksen ymmärtämisestä on tullut entistä tärkeämpää. Castelfranchi ja Tan (2002, 67) tuovat kuitenkin esille, ettei luottamus synny pelkästään teknologiaa parantamalla. He tähdentävät - Zhun

ym. (2011) teknologisen luottamuksen sijaan - ihmisten välisiä yhteisiä tietoja, asenteita ja sääntöjä. Ne on kuitenkin heidän mielestä integroitava teknologiaan, koska entistä enemmän kanssakäyminen verkossa tapahtuu jopa pelkästään teknologian kanssa ns. keinotekoisten ihmisten kanssa. (Castelfranchi ja Tan 2002, 57, 66.)

Kuzheleva-Sagan ja Suchkova (2016, 381) ovat tutkineet suhdetoiminnan (PR:n) ja graafisen suunnittelun vaikutusta luottamuksen syntymiseen internetissä. He sovelsivat tutkimuksessa Sztompkan (2012) luottamuksen kolmitasoisuutta ja tulosten perusteella suhdetoiminta sijoittui toiselle ja kolmannelle luottamuksen tasolle, koska sen avulla voitiin vaikuttaa avoimuuteen ja sisältöön. Suhdetoiminnan avulla voidaan pyrkiä mm. minimoimaan verkkopalveluiden käyttäjien riskin tunnetta ja luoda lisäarvoa erilaistumalla kilpailijoihin nähden sekä kehittää verkkopalveluiden toiminnallisuutta. Luottamusta voi myös lisätä tekemällä erilaisia sisältöjä eri tavoilla - ei vain verkossa. (Kuzheleva-Sagan ja Suchkova 2016, 384, 389.) Tämän perusteella voidaan sanoa, että graafinen ilme ja suhdetoiminta vaikuttavat merkittävästi luottamukseen organisaatiota kohtaan.

Kuzheleva-Sagan ja Suchkova 2016, 384) on myös sitä mieltä, että luottamus on osa ihmisyyttä ja siten välttämätöntä ja osa yhteiskuntaa. Kansainvälisen markkinointiviestinnän yrityksen Edelmannin tutkimus (2017) on kuitenkin osoittanut, että osassa maita luottamus yhteiskuntaan ja sen instituutioihin on vähentynyt. Edelmanin (2017) tutkimukseen viitaten Ries (2017) on blogikirjoituksessaan tuonut esille, että jos ihmiset eivät luota enää maan instituutioihin, julkisiin tahoihin ja mediaan, niin jonkun on täytettävä epäluottamuksen ”aukko” ja silloin sen täyttämiseen tarvitaan luotettavia organisaatioita. Tähän viittaa myös Bersoff (2017), joka blogikirjoituksessaan neuvoo organisaatioita keskittymään erityisesti mittaamaan luottamustaan, monitoroimiaan mainetta, mutta lisäksi tekemään kaikkensa lisätäkseen luottamusta.

Samaa mieltä luottamuksen vähenemisestä yhteiskunnassa ovat myös Dasgupta ja Ferebee (2013, 58), joiden mielestä luottamuksen ja avoimuuden aika on pian verkossa ohi ja vaarana on, että internet hajaantuu osiin ns. kansakuntien ja organisaatioiden välisiin yhteistyöverkostoihin. He peräänkuuluttavat avoimuuden ja yhteistyön lisäämistä yli maantieteellisten rajojen niin kansakuntien kuin organisaatioidenkin välillä. Vaarana on, että jos luottamus ja avoimuus katoavat, on sillä vaikutus maailmanlaajuiseen talouteen (Dasgupta ja Ferebee 2013, 61, 63).

Koska tutkimuksessa ei ole tarkoitus selvittää SaaS-organisaatioiden sidosryhmien luottamusta, keskitytään työssä ensisijaisesti organisaation luotettavuuteen. Käsitteiden läheisyydestä johtuen pidettiin kuitenkin tärkeänä käsitellä ja määritellä myös luottamus tähän työhön.

Digitaalinen luottamus *on ulkoiseen sidosryhmään kuuluvan henkilön tunne, joka syntyy luotettavuuden seurauksena organisaatiota kohtaan, mutta joka vaatii pitkäjänteisyyttä ja aikaa.*

2.6 Maine

SaaS-organisaatiot, joista moni toimii vain digitaalisessa ympäristössä, verkkomaineen merkitys on tärkeä. Mainetta määritellään monella tapaa ja on useita mielipiteitä, mitkä tekijät vaikuttavat siihen. Yhteistä määritelmissä on se, että maine on aina seurausta jostakin.

Osa tutkimuksista on sitä mieltä, että organisaation vastuullisuudella ja sen viestimisellä on vaikutus maineeseen. Tran, Ngyuen, Melewar ja Bodoh (2015) tuovat esille, että varsinkin verkossa olevilla organisaatioilla on erityisen tärkeää luoda hyvä yrityskuva ja panostaa viestintään, jolla lisätään luottamusta. Se tarkoittaa sosiaalisen vastuun ja eettisen toiminnan esille tuomista eli sitä, mitkä ovat organisaation arvot (Tran ym. 2015, 98.) Myös luottamuksella ja hyvällä yrityskansalaisuudella sekä toimialaa koskevilla uutisilla oli heidän tutkimuksen mukaan merkitystä yrityskuvan muodostumiselle (Tran ym. 2015, 102.) Vastuullisuus on osa mainetta myös Fombrunin (1996, 136) mielestä, mutta se koostuu hänen mukaan sen lisäksi omaperäisyydestä verrattuna kilpailijoihin.

Lisäksi maineeseen vaikuttaa, koetaanko organisaation arvot ja ominaisuudet läheisiksi (Coombs ja Holladay 2015, 692.) Organisaation arvojen tulee vastata sekä liiketoimintaa että merkityksellisten sidosryhmien arvoja (Hatch ja Shultz 2003, 1058). Coombsin ja Holladayn (2015, 692) tutkimuksessa on myös nähty tärkeäksi, tunnetaanko organisaation kanssa samankaltaisuutta tai halutaanko esimerkiksi tavoitella samankaltaista identiteettiä, mikä organisaatiolla on. Arvoihin ja toimintaan kannattaakin kiinnittää huomioita, sillä organisaation toiminnasta kumpuavat ja nopeasti internetissä leviävät skandaalit, huhut, kommentit, palautteet ja vastaukset vaikuttavat myös maineeseen (Falkheimer 2014, 127).

Ylipäätään ulkoisella viestinnällä ja sen tehokkuudella ja kokemuksilla on vaikutus maineeseen. Correian, Kaufmannin ja Rabinon (2014) tutkimus osoitti, että viestintä vaikuttaa asiakkaan saamaan arvoon, joka puolestaan vaikuttaa tyytyväisyyden kautta organisaation maineeseen. Asiakkaan saama arvo vaikutti myös suoraan siihen, miten organisaation luotettiin ja sitouduttiin, ja niihin taas vastaavasti vaikutti organisaation maine (Correia ym. 2014, 198). Myös Coombs ja Holladay (2015, 692) liittävät asiakkaan tyytyväisyyden parempaan maineeseen. Asiakastyytyväisyyteen vaikuttaa asiakaskokemukset ja Tran ym. (2015, 103) ovatkin sitä mieltä, että kokemuksista tulisi tehdä positiivisesti mieleenpainuvia ja niiden tulisi olla linjassa organisaation toiminnan ja viestinnän kanssa. Pilvipalveluissa, joita myös SaaS-palvelut ovat, mainetta pidetään luottamuksen seurauksena, johon vaikuttavat sekä omat että suosittelijoiden kokemukset palveluiden käytöstä (Sarojini 2015, 2). Kokemuksiin ja viestintään voidaan liittää myös seuraavat maineeseen vaikuttavat tekijät: organisaation ulkoinen ilme (mm. verkkosivujen ulkoasu), verkkosivujen käytettävyys ja sisältö, digitaalinen läsnäolo ja esiintyminen, henkilöstön esiintyminen, asenne ja käyttäytyminen (mm. avuliaisuus) (Tran ym. 2015, 102.) Kaiken kaikkiaan organisaation digitaalisella läsnäololla voidaan nähdä olevan iso merkitys organisaation maineelle.

Osa organisaation mainetutkimuksista pitää mainetta enimmäkseen sidosryhmien kautta syntyvänä ja osa sen lisäksi jokaisen subjektiivisena kokemuksena. Esimerkiksi Fombrun (1996) ja Gotsi ja Wilson (2001) ovat sitä mieltä, että mielikuva ja sitä kautta syntyvä organisaation maine vaihtelevat eri sidosryhmillä, riippuen siitä, miten luotettavana, uskottavana ja vastuullisena organisaatiota pidetään (Fombrun 1996, 37, 80; Gotsi ja Wilson 2001, 28). Myös Hatchin ja Shultzin (2003, 1044, 1047-1048) mukaan mielikuva rakentuu viime

kädessä aina jokaisella yksilöllä subjektiivisesti, vaikka organisaatio vaikuttaakin mielikuvien syntymiseen, halusipa tai ei.

Gotsi ja Wilson (2001) ovat tarkastelleet omassa tutkimuksessaan useita mainetta käsitelleitä tutkimuksia ja lähteiden perusteella he ovat määritelleet yrityksen maineen seuraavasti:

> "*Sidosryhmien kokonaisvaltaiseksi arvioinniksi organisaatiosta, joka on syntynyt ajan myötä ja siinä yhdistyy sidosryhmien omat kokemukset, organisaation viestintä ja visuaalinen ilme ja teot sekä organisaation toimet suhteessa sen kilpailijoihin.*" (Gotsi ja Wilson 2001, 29).

Edellisten määritelmien tavoin se sisältää sidosryhmien arvioinnin, mutta myös aikakäsityksen ja vuorovaikutuksen. Maine ei synny hetkessä vaan se vaatii aikaa, ja toiseksi maine muodostuu vuorovaikutuksessa yhdessä organisaation ja sen sidosryhmien välillä. Myös Gurau (2013) liittää maineeseen vuorovaikutuksen eli organisaation maine syntyy, "*miten asiakkaat ymmärtävät ja vastaavat organisaation toimiin ja keskusteluun*" (Gurau 2013, 523.). Siten voidaankin sanoa, että maine syntyy sekä organisaation oman, mutta myös sen sidosryhmien viestinnän seurauksena eli yhdessä käytävässä vuorovaikutuksessa.

Maine liitetään myös turvallisuuteen. Sarojinin (2015) artikkelista voidaan poimia ajatus, että palveluntarjoajan maineella on merkitystä ja hyvä maine kertoo mm. turvallisuudesta; mitä parempi maine, sitä turvallisempana palvelun käyttöä voidaan pitää.

Edellä puhuttiin lähinnä maineen saavuttamisesta, mutta on tärkeää tuoda lyhyesti esille myös maineen ylläpitäminen. Maineen säilyttämisessä pidetään tärkeänä sekä organisaation sisäisiä, että ulkoisia sidosryhmiä. Fombrun (1996, 67) mielestä "*luottamuksen rakentaminen työntekijöihin säilyttää organisaation maineen.*" Se tarkoittaa mm., että henkilökuntaan luotetaan, heitä kannustetaan ja pyritään olemaan ylpeitä omasta työstään (Fombrun 1996, 136.) Organisaation ulkopuolella se tarkoittaa vastaavasti lupauksien pitämistä (Fombrunin 1996, 28, 32, 72.). Lisäksi Correian, Kaufmannin ja Rabinon (2014, 189) mukaan organisaation on pystyttävä pitämään lupaukset maineen säilyttämiseksi.

Maineen yhteydessä puhutaan usein myös maineenhallinnasta (reputation management). Sen avulla organisaatio voi pyrkiä vaikuttamaan mielikuviin ja maineeseen, joita se synnyttää, vaikka maineen katsottaisiinkin syntyvän vuorovaikutuksessa sidosryhmien kanssa ja, sidosryhmien määrittelevän lopullisen maineen. Jokaisella organisaatiolla on kuitenkin omat tavat, joilla se pyrkii luomaan mainettaan (Fombrun 1996, 72).

Tässä tutkimuksessa organisaation maine määritellään seuraavasti.

Organisaation maine kyberympäristössä *rakentuu mielikuvista, luotettavuudesta, uskottavuudesta ja vastuullisuudesta sekä vuorovaikutuksesta sidosryhmien kanssa digitaalisessa ympäristössä. Lisäksi siihen vaikuttaa organisaation läsnäolo ja viestintä, mutta myös sidosryhmien ja suosittelijoiden kokemukset.*

2.7 Organisaatioviestintä kyberympäristössä

Tässä tutkimuksessa organisaatioviestintä nähdään ns. integroituna viestintänä, jossa yhdistyy Rielin ja Fombrunin (2007, 14) ajatus, että kaikenlainen organisaation viestintä yhdistää kaikki sidosryhmät organisaation, ja Grigorescun ja Lupun (2015, 71) näkemys, että koko

organisaation viestintä tukee strategiaa, ja ulkoinen sekä sisäisen viestintä liittyvät kiinteästi toisiinsa. Organisaatioviestinnän tavoitteena nähdään tässä työssä Grigorescun ja Lupun (2015, 71) tavoin organisaation menestyminen pitkälle tulevaisuuteen.

Vaikka organisaatioviestintä nähdään tässä tutkimuksessa integroituna viestintänä, keskitytään silti ensisijaisesti ns. ulkoiseen viestintään ulkoisten sidosryhmien kanssa. Silti ei täysin voida unohtaa sisäistä viestintää. Esimerkiksi sisäisen viestinnän perinteinen merkitys mm. saada henkilökunta ymmärtämään ja sitoutumaan organisaation strategiaan ja voimaan hyvin (Riel ja Fombrun 2017, 188) liittyy nykyisin vahvasti ulkoiseen viestintään, koska kyberympäristön johdosta työntekijät voivat, ja usein ovat myös kannustettuja, olemaan suoraan yhteydessä ulkoisiin sidosryhmiin (Cornelissen 2017, 36). Silloin on tärkeää, että sisäisellä viestinnällä on luotu yhteiset tavat ja tavoitteet, sillä organisaation henkilökunnalla ja sen verkkoläsnäololla on enenevä merkitys yrityksestä muodostuvaan mielikuvaan. Henkilökunnan viestinnän tulisikin olla yhdenmukaista organisaation muun viestinnän kanssa verkossa (Tran ym. 2015, 104.) Johdonmukaisuuteen kannattaakin kyberympäristössä kiinnittää huomioita, sillä verkkoviestinnällä on keskeinen rooli organisaation maineen muodostumisessa (Foroudi ja Montes 2017, 206).

2.7.1 Kolme eri viestintäkeinoa kyberympäristöön

Viestintä ja vuorovaikutus ovat muuttuneet paljon parinkymmenen vuoden aikana. Koko organisaation toimintaan ja olemassaoloon on viestinnällä suuri merkitys ja kyberympäristö ja teknologia ovat tehneet viestinnästä tehokasta ja laajentaneet mm. vuorovaikutuksen eri foorumeita (Falkheimer 2014, 125). Yksi iso muutos foorumeiden lisääntymisen lisäksi on kanssakäymisen lisääntyminen koneiden ja laitteiden kanssa ja ihmisten välinen vuorovaikutus tapahtuu usein tietämättä mitään vastapuolesta (Kuzheleva-Sagan ja Suchkova 2016, 382).

Foroudi ja Montes (2017, 201-202) kutsuvat organisaation digitaalista verkkoviestintää (corporate e-communication) ”*digitaaliseksi vuorovaikutukseksi, joka organisaatiolla on sen sidosryhmien kanssa*.” Digitaalisesta viestinnästä kyberympäristössä eri muodoissaan on tullut keskeinen osa organisaatioiden viestintää ja siellä toimimiseen organisaatiolla tulee olla strategiatason joustavuutta, koska verkostoissa kilpailu on kovaa (Spagnoletti, Za ja D’Atri, 2007, 1).

Cornelissen (2017, 42-43) on jakanut organisaation olemisen digitaalisessa ympäristössä kolmeen erilaiseen kategoriaan, mediaan. Taulukko 3 on muunnelma Cornelissenin jaottelusta, ja nämä eri mediat voidaan hyvin nähdä myös Foroudin ja Montesin (2017) organisaation digitaalisena vuorovaikutuksena. Nämä kaikki mediamuodot ovat keskeisiä myös organisaatioviestinnässä, ja pärjätäkseen millä tahansa mediakentällä, tarvitaan ketteryyttä ja strategiaa. Tässä työssä keskitytään lähinnä omaan mediaan, mutta jonkin verran myös ansaittuun mediaan.

TAULUKKO 3. Organisaation mediat digitaalisessa ympäristössä (mukaelma Cornelissenin taulukosta 2017, 42)

Mediat	Ilmeneminen	Tehtävä /Tavoite	Edut	Haitat
oma media	Organisaation verkkosivut, blogit, sometilit eri somekanavissa.	Sidosryhmien sitouttaminen ja suhteen vahvistaminen.	Kontrolli, mahdollisuus sitouttaa sidosryhmiä.	Ei ole varmuutta sitouttamisesta. Voi herättää epäilyjä organisaatiota kohtaan.
ostettu media	Sponsorointi ja mainokset.	Organisaation ja / tuotteiden mainonta, näkyvyyden lisääminen.	Kontrollin mahdollisuus.	Ei uskottavuutta maksettuna.
ansaittu media	Nettipuskaradiokeskustelu, aineiston jakaminen muun kuin organisaation toimesta.	voi olla seurausta toiminnasta omassa ja ostetussa mediassa tai voi ostetun median kautta johtaa suurempaan viestintään omassa mediassa. Sidosryhmäsuhteiden vahvistaminen.	Uskottavinta ja luotettavinta, vahvinta sidosryhmien sitouttamista.	Ei kontrollia, voi olla negatiivista keskustelua, muunneltuja mainoksia negatiivisessa tarkoituksessa.

Varsinkin niillä yrityksillä, jotka toimivat vain internetissä, on erityisen tärkeää, millainen niiden läsnäolo, näkyminen ja toiminta on kyberympäristössä. Yhtä tärkeää on kuitenkin ymmärtää myös sidosryhmiä ja sitä, miten he haluavat organisaatioiden olevan läsnä verkossa. Kun sidosryhmät kokevat mm. organisaation toimivan verkossa vastuullisesti ja eettisesti, organisaatio voi lisätä sidosryhmien sitä kohtaan tuntemaa luottamusta (Tran ym. 2015, 103). Mutta myös mediamuodolla on vaikutusta sidosryhmien sitouttamiseen, kuten taulukosta kolme voidaan nähdä. Koska oman median kautta on mahdollisuus sitouttaa sidosryhmiä, on tärkeää, että panostetaan viestintään ja huomioidaan sidosryhmät. Kuten aiemmin on jo mainittu, organisaatio ei voi täysin hallita mainettaan, mutta viestinnän ja maineenhallinnan avulla se voi pyrkiä mm. vaikuttamaan ansaittuun mediaan.

2.7.2 Laajasti läsnä eri kanavissa

Organisaation medioissa (Cornelissen 2017) ja siten digitaalisessa viestinnässä mm. sosiaalinen media on yksi tärkeimmistä vuorovaikutusverkostoista sidosryhmien ja organisaatioiden välillä (Foroudi ja Montes 2017, 201, 203). Sosiaalisen median yhteydessä puhutaan ns. keskusteluareenoista (issue arenas), jotka Luoma-Aho ja Vos (2010, 316, 319) käsittävät digitaalisiksi vuorovaikutuksen areenoiksi. Vernuccion (2014) mielestä sosiaalinen media on erilaisten keskusteluareenojen kenttä eli se tarkoittaa niitä sovelluksia, joita käytetään internetin välityksellä, joissa toiminta perustuu keskinäiseen vuorovaikutukseen, sisällön jakamiseen ja luomiseen (Vernuccio 2014, 214). Sosiaalinen media käsittää erilaisia yhteisöpalveluja (esim. Facebook, Youtube, Instragram, Pinterest, Flickr), blogialustoja (henkilökohtaisia ja organisaatioblogeja), chat-sovelluksia (esim. SnapChat) tai ovat niiden yhdistelmiä,

kuten Twitter, ja sen lisäksi on virtuaalimaailmoja (esim. Second Life ja erilaisia keskustelupalstoja) (Vernuccio 2014, 214-215). Mutta on muistettava, että sosiaalisen median kanavien lisäksi digitaalista viestintää internetissä ovat organisaatioiden verkkosivut, sähköpostit ja erilaiset suljetut sidosryhmäkanavat ja alustat sekä tässä työssä SaaS-organisaatioiden palvelut. Cornelissenin (2017) jaottelun mukaisesti nämä kaikki kuuluvat organisaation omaan mediaan.

2.7.3 Viestintä osaksi strategiaa

Kuten edellä kävi ilmi, on sosiaalinen media tärkeimpiä viestinnällisiä verkostoja sidosryhmien ja organisaatioiden välillä (Foroudi ja Montes 2017, 201, 203). Jotta erilaiset sidosryhmät, joihin suhde on muuttunut kyberympäristön myötä entistä hauraammaksi ja vaikeaselkoisemmaksi, voidaan huomioida paremmin, tulisi viestinnän olla osa strategiaa. Strateginen viestintä on tärkeää myös siksi, että vuorovaikutusareenat ovat lisääntyneet ja viestinnän merkitys kasvanut (Falkheimer 2014, 126, 128). Strategisen viestinnän avulla pystytään kaikista parhaiten vaikuttamaan organisaation vuorovaikutukseen, olemassaoloon ja toimintaan (Falkheimer 2014, 128).

Samaa mieltä on viestinnän ammattilaisten järjestö ProCom (2012). Kun viestintä on osa strategiaa, niin se on silloin myös luomassa arvoa ja on "*olennainen osa yrityksen arvoketjua*" (Zerfass ja Viertmann 2017, 72). Viestinnän tulisi siis luoda arvoa sille, mikä strategian kannalta on sillä hetkellä tärkeintä. Tulisikin olla vuoropuhelua sekä organisaation sisällä, että ulkoisten sidosryhmien kanssa, avoimesti ja rehellisesti. (ProCom 2012). Samaa mieltä on Falkheimer (2014, 130-131), joka näkee, että strategisesti johdettu viestintä lisää avoimuutta organisaatiossa, mutta myös ulkoisessa viestinnässä.

Toimivaan vuoropuheluun tarvitaan ymmärrystä siitä, mitä sidosryhmät milloinkin tarvitsevat ja haluavat. Siihen tarvitaan monitorointia eli ilmaisujen ja odotusten selvittämistä. Sen lisäksi tarvitaan muutosnopeutta tarpeeseen vastaamiseen (ProComin 2012.). Strategisesti johdettu viestintä luo raamit näille eli, miten kyberympäristössä toimitaan, mitä keskusteluja seurataan ja ketkä osallistuvat vuorovaikutukseen. Lisäksi sen avulla tehdään suunnitelmat viestinnän säännöllisyydestä. Palveluiden eli esimerkiksi SaaS-palveluiden tarjonnan kasvaminen yhteiskunnassa vaatii myös strategista viestintää, koska suhteiden hoitamisella, organisaation arvoilla ja palautteisiin reagoimisella on vaikutusta yrityskuvaan. (Falkheimer 2014, 127.) Sitä kautta voidaan vaikuttaa luottamukseen organisaatiota kohtaan. (Falkheimer 2014, 130-131.)

2.7.4 Aitoa keskustelua ja odotuksiin vastaamista

Organisaatioviestinnän näkökulmasta sosiaalinen media keskusteluareenoineen on mahdollistanut uuden tavan tuottaa ja jakaa sisältöä sekä osallistua keskusteluun niin sidosryhmien kuin ison yleisön kanssa (Vernuccio 2014, 214). Vuorovaikutus varsinkin sosiaalisen median kanavissa tarkoittaa nimenomaan keskustelua, vuoropuhelua ja toisaalta myös sitä, ettei se ole täysin, jos lainkaan, organisaation hallittavissa (Luoma-Aho ja Vos 2010, 322). On oltava ketterä, mutta silti luotava erilaisia sosiaalisen median strategioita eri areenoille, sillä kaikki ei käy kaikkialle. On tiedettävä, miksi milläkin areenalla ollaan, mikä on tarkoitus ja mihin siellä pyritään vaikuttamaan (Luoma-aho ja Vos 2010, 323-324). Organisaation on oltava aktiivinen ja keskusteltava sen sidosryhmien kanssa siellä, missä he ovat ja mistä he keskustelevat.

Toisaalta Coombs ja Holladay (2015) tuovat esille, että sosiaalisessa mediassa ei ole todellista sidosryhmien välistä vuorovaikutusta, kun viestintää voi tehdä ilman nimeä, jolloin siitä tulee vähemmän tasa-arvoista tai tasapuolista. Vuorovaikutuksen tulisi perustuakin siihen, että tiedetään, kenen kanssa keskustellaan ja nimenomaan keskustellaan, eli mm. vastataan viesteihin (Coombs ja Holladay 2015, 691.)

Vuorovaikutus tarkoittaa keskustelun ja vastaamisen lisäksi myös sidosryhmien neuvontaa (Vernuccio 2014, 216, 227). Kun kyseessä on auttaminen, voidaan uskoa, että sellaisen sisältö kiinnostaa sidosryhmiä, mutta kiinnostavan sisällön lisäksi tulisi Vernuccion (2014) mielestä huomioida myös sisällön laatu, ja, että se on tehty sellaisille kohderyhmille, joita halutaan tavoittaa. Tekstimuodossa olevan keskustelun lisäksi tulisi vuorovaikutukseen käyttää esimerkiksi videoita, livetoistopalveluita ja podcasteja. (Vernuccio (2014, 216.)

Navarron, Morenan ja Al-Sumaitin (2017, 706) mukaan viestinnän ammattilaiset eivät kuitenkaan tarpeeksi huomioi viestinnässään sidosryhmien odotuksia sosiaalisessa mediassa, vaan tekevät sitä edelleen liian paljon omista lähtökohdistaan. Tulisikin ottaa selvää sidosryhmien odotuksista ja pyrkiä täyttämään odotukset, sillä siten organisaatio parhaiten edistää mainetta, olemassaoloaan ja luottamusta sitä kohtaan (Olkkonen ja Luoma-aho 2005, 93).

Monitorointi on keino selvittää odotuksia. Monitoroinnin tulisikin olla keskeinen viestinnän tehtävä, koska digitaalinen ympäristö on nykyisin sidosryhmäsuhteiden ja ylipäätään viestinnän yksi tärkeimmistä toiminta-alueista (Strauβ ja Jonkman 2017, 35). Se on merkityksellistä myös siksi, että, moni tekee päätöksen organisaation palvelun tai tuotteen käytöstä pelkästään digitaalisesta ympäristöstä saadun tiedon valossa. Lisäksi digitaalisessa ympäristössä kriisit syntyvät ja laajenevat nopeasti (Strauβ ja Jonkman 2017, 34), mutta monitoroinnilla ennakointi ja kriisien syntymisen ehkäiseminen on mahdollista. Näiden lisäksi monitoroinnin tuloksena voi seurauksena olla jopa organisaation strategian muuttaminen enemmän sidosryhmien odotusten mukaiseksi. Nykyään seurantaa voi myös tehdä isossa mittakaavassa tehokkaasti teknologia-avusteisesti eli hyödyntämällä ns. big dataa (Strauβ ja Jonkman 2017, 34).

2.7.5 Suhteiden vahvistamista

Monitorointi on myös keino vahvistaa suhteita. Slabbertin ja Barkerin (2014, 92) mallissa sidosryhmäsuhteiden vahvistamisesta yhdistyvät vuorovaikutuksellinen ja integroitu viestintä organisaation ja sidosryhmien välillä sekä monitorointi. Merkittävintä mallissa on, että sidosryhmät osallistuvat tasavertaisena organisaation maineen rakentamiseen. Mallin mukaan suhteiden vahvistaminen vaatii myös monitorointia, eli seurantaa siitä, mistä sidosryhmissä keskustellaan ja mikä heitä kiinnostaa (issues management), tärkeiden sidosryhmien tunnistamista ja heidän odotusten selvitystä. Jotta suhteista tulisi mahdollisimman kestävät, tarkoittaa se myös sitä, että on tehtävä jatkuvaa arviointia ja selvitystä, kuinka hyvin viestintä vastaa sidosryhmien tarpeita ja odotuksia ja mitä asioita nousee esille heidän kanssa käytävässä vuorovaikutuksessa. Kaikesta sidosryhmien huomioimisesta huolimatta viestinnän tulee kuitenkin pohjautua organisaation kulttuuriin ja arvoihin (Slabbert ja Barker 2014, 92). Sidosryhmäsuhteiden vahvistaminen ja kehittäminen vaatii aikaa, panostusta, viestinnän osaamista, kykyä havaita ns. vihjeitä ja mahdollisuutta reagoida nopeasti (Slabbert ja Barker 2014, 93). Kuten huomataan, sidosryhmäsuhteiden vahvistamisen yhteydessä käytetään hyvin pitkälle samoja määreitä, joita tuli esille maineen, luotettavuuden ja luottamuksen yhteydessä.

Shinin, Pangin ja Kimin (2015, 185) tutkimuksessa kuitenkin kävi ilmi, ettei organisaatiot käytä digitaalista viestintää sitouttamiseen vaan viestintä erilaisesta ympäristöstä huolimatta on edelleen pitkälti yksisuuntausta sisällöntuottamista eikä niinkään todellista keskustelua. (Shin ym. 2015, 200.) Heidän ehdotus vuorovaikutuksen lisäämiseen ja sitouttamiseen on esimerkiksi, että organisaation internetsivuille luodaan mm. sidosryhmälähtöistä sisältöä ja luodaan linkit kaikkiin sosiaalisen median kanaviin, joissa sidosryhmäläiset voivat keskustella, kysyä ja kommentoida. Facebookissa vuorovaikutusta voi lisätä mm. esittämällä avoimia kysymyksiä ja jättämällä lauseita avoimiksi. Twitterissä ja Facebookissa, vuorovaikutus lisääntyy pelkästään vastaamalla asiakkaille, mutta hyödyntämällä hastageja ja linkkejä ja jakamalla hyödyllistä tietoa, voidaan myös lisätä vuorovaikutusta ja sitoutumista (Shin ym. 2015, 211-212.) Aiemmin mainittiin Vernuccion (2014) keinoja vuorovaikutuksen lisäämiseen (mm. neuvontaa, sisällön laatuun panostamista ja monipuolisten kanavien ja keinojen käyttämistä (Vernuccio 2014, 216, 227), joilla myös nähdään olevan mahdollisuus vaikuttaa sidosryhmien sitoutumiseen.

2.7.6 Ennakointia ja rehellisyyttä

Henrik Rydenfelt (2014, 41) on sanonut, että organisaatioviestinnässä on vallalla ennakointi ja proaktiivisuus entisen reagoinnin sijaan. Hän on myös sitä mieltä, että vain pahimpaan varautuminen ei ole proaktiivisuutta vaan lisäksi se *"…tarkoittaa nykyisessä toimintaympäristössä myös omaehtoista ongelmien esiintuontia, viestintää."* (Rydenfelt 2014, 44).

Tuosta Rydenfeltin ajatuksesta on jo neljä vuotta, mutta silti kyberturvallisuusuhkien onnistuneista iskuista ollaan monesti hyvin hiljaa eikä niitä tuoda omaehtoisesti esille, vaikka myös viestintäviraston kyberturvallisuuskeskuksen tietoturva-asiantuntija Perttu Halosen mukaan niistä nimenomaan pitäisi kertoa. Kun kyberturvallisuusiskut ja -uhkat tuodaan julkisuuteen, niitä vastaan pystytään paremmin puolustautumaan (Yle 6.3.2018). Hyvä esimerkki ongelmien oma-aloitteisesta julkisuuteen tuomisesta on metsäyhtiö Metsä Group, joka ilmoitti 9.1.2018 epäilevänsä, että yritys on joutunut tietomurron kohteeksi (HS 9.1.2018). Osasyy asian julkaisemiseen saattoi johtua siitä, että yritys epäili tulostietojen joutuneen vääriin käsiin, ja pörssiyhtiönä tulostietojen julkistaminen on säädelty, jos tiedoilla katsotaan olevan vaikutusta osakekurssiin. Toivottavasti kyse oli kuitenkin myös viestinnän proaktiivisuudesta. Metsä-Groupin lisäksi julkisuuteen tuli SaaS-palveluita tarjoava Provincia, mutta vasta haittaohjelman iskiessä sen palveluihin eli vasta, kun kriisi oli päällä. Silti viestintävirasto piti yrityksen toimintaa esimerkillisenä, sillä kertomalla kyberturvallisuusiskusta, moni muu pystyi suojautumaan haittaohjelmaa vastaan (Yle 6.3.2018). Voidaan kuitenkin kysyä, kuinka moni muu kyberturvallisuusisku olisi epäonnistunut tai tyrehtynyt alkuunsa, jos viestintä olisi ollut proaktiivista ja avointa?

2.7.7 Ammattimaista sidosryhmäviestintää omalla tavalla

Limnéll ym. (2014) tuo esille kyberstrategian yhteydessä mahdollistamissuunnitelman, joka on lyhyesti sanottuna osa strategiaa, ja sisältää toimivat suunnitelmat ja tehtävät kybermahdollisuuksille. Mahdollistamissuunnitelma koostuu mm. sosiaalisesta pääomasta, joka käsittää maineen, ansaitun tietoisuuden ja asiakkaan. Tulisi miettiä, miten näihin sosiaalisen pääoman alatekijöihin voidaan vaikuttaa, ettei kybermahdollisuuksista tulisi kyberuhkia. Maineen osalta Limnéll ym. (2014) toteavat, että organisaation toiminnan tulisi olla johdon-

mukaista, jotta maine olisi mahdollisimman hyvä. Suunnitelmassa korostetaan myös monitorointia ja proaktiivisuutta. On osallistuttava vuorovaikutuksen, jotta voi pyrkiä paremmin vaikuttamaan kyberympäristössä olevaan keskusteluun ja varautumaan uhkiin. Ansaitulla tietoisuudella tarkoitetaan lähinnä vuoropuhelua eli organisaatio voi omilla toimillaan vaikuttaa osittain siihen, mitä sisältöä jaetaan, missä yhteyksissä ja miten organisaatioon reagoidaan. Asiakkaan tuomisella liiketoiminnan ytimeen taas tarkoitetaan sitä, että organisaatio tekee sidosryhmälähtöistä viestintää ja pyrkii luomaan tyytyväisyyttä, mutta myös löytämään uusia sidosryhmiä. (Limnéll ym. 2014, 18, 181,186, 187.)

Mahdollistamissuunnitelma kuulostaa strategiselta sidosryhmälähtöiseltä viestinnältä. Voidaankin sanoa, että viestintä kyberympäristössä vaatii mm. viestinnänosaamista ja aikaa (Slabbert ja Barker 2014, 93) sekä strategiatason suunnitelmallisuutta (Falkheimer 2014, 126), mutta myös sidosryhmälähtöisyyttä (Olkkonen ja Luoma-aho 2005, 93). Näiden avulla voitaisiin ehkä saavuttaa Pangin, Shinin, Lewin, ja Waltherin (2018, 77) ns. ihannetilanne, jossa organisaation ympärille kyberympäristöön muodostuisi yhteisöjä (omissa medioissa tai ansaituissa medioissa), joissa sidosryhmät kokisivat saavansa tukea, apua ja kokisivat tulevansa kuuluksi ja joissa syntyisi aitoa vuorovaikutusta, ei vain organisaation, vaan myös muiden sidosryhmien ja yhteisöön kuuluvien kanssa. Näistä virtuaaliyhteisöistä voisi muodostua vahvoja ja avoimia yhteisöjä, josta hyötyisivät kaikki. (Pang ym. 2018, 77.)

Gurau (2013) on kuitenkin oman verkkokampanjoihin keskittyneessä tutkimuksensa havainnut, ettei ole yhtä ainoaa tapaa, jolla organisaatio voi menestyä verkkoympäristössä. Aina se vaatii organisaatiolta jo aiemmin mainittua nopeaa reagointikykyä ja sopeutumiskykyä, mutta myös rehellisyyttä. (Gurau 2013, 534). SaaS-organisaation olisikin hyvä tehdä strateginen päätös Cornelisenin (2017, 42) medioiden käyttämisestä, jotka tukisivat sitä päämäärien, sidosryhmien ja tilanteiden mukaisesti.

Tässä tutkimuksessa kyberympäristössä tavoiteltavan organisaatioviestinnän määritelmä on seuraava.

Tavoiteltava organisaatioviestintä kyberympäristössä *lähtee organisaatioon arvoista ja kulttuurista ja on osa strategiaa. Viestintä on nopeaa ja joustavaa ja perustehtäviin kuuluu ympäristön monitorointi ja proaktiivisuus. Sen tavoitteena on organisaation menestymisen turvaaminen ja sidosryhmien yhdistäminen ja sitouttaminen. Nämä tavoitteet organisaatio saavuttaa olemalla todellisessa vuorovaikutuksessa sidosryhmien kanssa, viestimällä johdonmukaisesti, luotettavasti rehellisesti ja avoimesti sekä sidosryhmälähtöisesti monipuolisin keinoin eri kanavissa.*

2.7.8 Digitaaliset sidosryhmäverkostot

SaaS-palveluiden, niitä tuottavien ja käyttävien organisaatioiden ja muiden sidosryhmien kesken tapahtuu vuorovaikutusta ja viestintää. Ne muodostavat digitaalisia sidosryhmäverkostoja kyberympäristössä.

Digitaalisia sidosryhmäverkostoja voidaan kuvata hyvin toimijaverkkoteorialla, (Actor-Network theory) eli ANT:llä, joka ei kuitenkaan ole teoria vaan "*lähestymistapa tai tutkimussuuntaus*" (Kullman ja Pyyhtinen 2015, 109). Coreenin (2009, 16) mukaan se on ihmisten ja digitaalisten laitteiden vuorovaikutuksen tutkimista, mutta se sisältää myös eri ryhmien väliset verkostot, jotka voivat olla sekä fyysisiä että digitaalisia verkostoja. Olennaista on kuvata verkostossa olevien toimijoiden välisiä suhteita, vuorovaikutusta inhimillisten ja eiinhimillisten toimijoiden välillä, eikä käsitellä varsinaisia rakenteita (Kullman ja Pyyhtinen

2015, 109; Eriksson 2015, 40). Lisäksi on tärkeää selvittää, mitkä tekijät ovat niitä, jotka pitävät ilmiötä tai verkostoa yllä (Kullman ja Pyyhtinen 2015, 110, 118). Lähestymistapa sopii hyvin viestinnän tutkimiseen, koska viestintä on vuorovaikutusta ja merkitysten tulkitsemista (Littlejohn ja Foss 2009, 17).

ANT:ssä verkostot eli rihmastot ovat vuorovaikutuksen keskiössä eli tutkitaan, millaisia rihmastoja vuorovaikutus muodostaa (Telivuo 2015, 42). Tässä työssä rihmastoista käytetään nimitystä digitaaliset sidosryhmäverkostot, joissa vuorovaikutus SaaS-organisaatoissa tapahtuu. Verkostoille on ANT:n mukaan ominaista monimuotoisuus ja laaja-alaisuus, yhteyksien luominen ja jatkuva muuttuminen. (Eriksson 2005, 43-44). Rihmastoajatus perustuu siihen, että jokainen yksittäinen toimija on aina osa jotain toista verkostoa, ja kun useampia verkostoja kietoutuu toisiinsa, muodostuu niistä verkostojen maailma, rihmasto (Eriksson 2015, 40). Suuntauksen mukaan asioiden olemassaolo on sitä vahvempaa ja todellisempaa, mitä enemmän ne ovat linkittyneet toisiinsa (Latour 2005; Eriksson 2015, 112), eli verkostot ovat erilaisia keskenään ja osassa linkit ovat vahvempia ja toisissa heikompia (Kullman ja Pyyhtinen 2015, 116). Verkostot eivät ole myöskään staattinen tila vaan ne elävät koko ajan ja toimijat luovat verkostoissa uusia merkityksiä (Luppicini, 2014, 4).

Vuorovaikutusverkostoja muodostavat toimijat (spokesperson, macroactor, actor) tai toiselta nimeltään aktantit (Latour 2007, 30-31, 54, jotka ovat inhimillisiä tai ei-inhimillisiä (Kullman ja Pyyhtinen 2015, 117) ja niitä voi olla äärettömästi (Latour 2007, 40). Latourin (2007, 31, 33) mielestä mitään ryhmää tai verkostoa ei voi olla olemassa ilman ryhmän edustajaa (spokesperson), joka ns. puhuu ryhmän puolesta ja saa ryhmän olemaan ja toimimaan yhdessä. Eli verkostot ja niiden väliset ja sisäiset linkit eivät muodostu automaattisesti vaan ne vaativat työtä ja jonkun tekijän ns. välikäden toimijoiden välille (Latour 2005 37-42; Kullman ja Pyyhtinen 2015, 115). Suuntauksen mukaan toimijat ovat tasavertaisia riippumatta siitä, ovatko ne inhimillisiä tai ei-inhimillisiä (Latour 2007, 54). Macroactor eli ns. makrotason toimija on isossa mittakaavassa tai verkostossa oleva toimija (Latour 2007, 30). Toimijat eli actorit ovat taas kaikki ne, jotka toimivat verkostossa ja toisaalta taas ne muodostavat yhdessä yhden kokonaisuuden eli aktantin. Eli myös kokonaisuus, yksittäisen ihmisen tai organisaation tavoin, voi olla aktantti. (Kullman ja Pyyhtinen 2015, 117.)

Toiminto eli varsinainen vuorovaikutus (macroacting, acting) voi tapahtua näkemättä muita toimijoita, kuten kyberympäristössä pääsääntöisesti tapahtuu. Vuorovaikutus on aina erikoislaatuista eikä se ole siten yleistettävissä ja lisäksi se on aina erilaista eri toimijoiden välillä ja sen voimakkuus tai vahvuus vaihtelee. (Latour 2007, 199-202.) Jos verkostoissa tapahtuu muutoksia, esimerkiksi voimasuhteissa tai toimijoiden määrässä, ja nämä toiminnot ovat seurattavissa, puhutaan silloin käännöksestä (translation) (Ciustiniano ja Bolici 2012, 195; Latour (2007, 108; Coreen 2009, 17). Crafwordin (Rizer 2005, 1) mukaan ANT;n avulla voidaan tarkastella, kuinka ja millä keinoilla verkostojen sisällä mm. vahvistutaan uhkia vastaan ja ylläpidetään vakautta.

Vuorovaikutusverkosto tarvitsee kuitenkin vakautta ja luotettavuutta ollakseen aktantti tai yksi (Kullman ja Pyyhtinen 2015, 118). Tätä vakaata tilaa kutsutaan ANT:ssä mustaksi laatikoksi (black box). Se vallitsee aktanttien eli toimijoiden kesken, jolloin kaikki toimivat yhteen kestävästi ja luotettavasti. (Kullman ja Pyyhtinen 2015, 118, 124.) Latour (2007, 202) kuvaakin tilaa sellaiseksi, jossa yhdenkin tekijän muuttuminen toiseksi tai sen häviäminen voi johtaa odottamattomiin seurauksiin. Jotta toimijoiden väliset suhteet olisivat mahdollisimman horjumattomia, tarkoittaa se Kullmanin ja Pyyhtisen (2015, 118, 124) mukaan sitä, että suhteiden väliset esteet tai haitat tulisi saada poistettua. Käytännössä tämä

voisi esimerkiksi tarkoittaa sitä, että ihmisten vuorovaikutustaidot, laitteistot ja yhteydet tulisi olla mahdollisimman samankaltaisia, jotta ne muodostaisivat vahvoja sidosryhmäverkostoja.

Kuten nähdään, voidaan ANT:n avulla tarkastella SaaS -organisaatioiden vuorovaikutussuhteita ja viestintää eri sidosryhmien kanssa kyberympäristössä. Sen lisäksi sitä voidaan käyttää kyberturvallisuusuhkien analysointiin, sillä esimerkiksi haittaohjelmat ovat toimijoita, jotka muokkaavat kyberympäristöä ja, jotka luovat myös omia ympäristöjä (Balzacq ja Cavelty 2016, 176). Lisäksi esimerkiksi haittaohjelmat, virukset, madot, trollit vaikuttavat ihmisten käsitykseen kyberturvallisuudesta ja siitä, millaisia iskuja pidämme mahdollisena (Balzacq, ja Cavelty 2016, 176). Siten haittaohjelmat toimijoina luovat verkostoja, muokkaavat niitä, ja vaikuttavat verkostojen pysyvyyteen sekä mahdollisesti uusien verkostojen luomiseen.

Myös luotettavuutta voidaan tarkastella verkostoajattelun kautta, sillä se ei ole Kullmanin ja Pyyhtisen (2015, 114) esimerkin tavoin itsestään olemassa oleva vaan se nimenomaan syntyy luottamuksen tavoin vuorovaikutuksessa eri toimijoiden välillä, johon vaikuttaa ihmisten ja verkostojen sisäiset sekä ulkopuoliset tekijät. Toimijoiden suhteen muodostuminen hitaasti (Kullman ja Pyyhtinen 2015, 122) ei sovi nykyajan nopeasti rakentuviin digitaalisiin verkostoihin, mutta toisaalta luottamuksen (Maister, Green ja Galford 2012, 48) ja maineen (Gotsi ja Wilson 2001, 29) rakentuminen vaativat aikaa.

3 TUTKIMUKSEN TOTEUTUS

3.1 Tavoite ja tutkimuskysymykset

Tämän tutkimuksen tavoitteena on selvittää, kuinka kyberympäristössä toimivissa SaaS-organisaatioissa nähdään yhteys kyberturvallisuusuhkien, luotettavuuden ja maineen välillä ja miten luotettavuutta pyritään rakentamaan kyberympäristössä. Luotettavuus on keskeinen osa rakennettaessa kyberturvallisuutta ja mainetta ja organisaatioviestintä on vastaavasti keino rakentaa luotettavuutta. SaaS-organisaatioille luotettavuus kyberturvallisuudessa on liiketoimintaympäristöstä eli kyberympäristöstä johtuen äärimmäisen tärkeää.

Tutkimuskysymykset ovat:

1. Miten kyberturvallisuusuhkat liittyvät SaaS-organisaatioiden luotettavuuteen ja maineeseen?
2. Miten viestinnällä voidaan vaikuttaa organisaation luotettavuuteen kyberympäristössä?

Tutkimuskysymyksiin haettiin vastauksia laadullisella eli kvalitatiivisella tutkimusmenetelmällä, koska siinä tarkoituksena on tutkia kokonaisuutta ja koska, sillä saadaan monipuolinen aineisto, josta pystyy hakemaan monia merkityksiä ja erilaisia näkökulmia (Alasuutari 2011, 84). Aineisto kerättiin haastattelemalla SaaS-palveluita tuottavien organisaatioiden viestinnästä vastaavia henkilöitä.

3.2 Tutkimuksen rajaus

Laadulliselle tutkimukselle on ominaista, että tutkija vaikuttaa tutkimukseen. Tutkija esimerkiksi valitsee ja rajaa aiheen omista lähtökohdista (Kiviniemi 2015, 77-79), mutta tutkimusotos on perusteltava eli, miksi tutkitaan juuri niitä kohteita (Liamputtong ja Ezzy 2007, 46). Tutkimukseen haluttiin organisaatioita, jotka joko kokonaan tai enimmäkseen toimivat kyberympäristössä, koska sekä luotettavuus että kyberturvallisuus ovat liiketoiminnan

kannalta tärkeitä asioita digitaalisessa ympäristössä. Siksi kohdeorganisaatioiksi valikoituivat suomalaiset SaaS-palveluita tuottavat organisaatiot, joilla palvelu on verkkoympäristössä. SaaS-organisaatiot, joihin päätettiin ottaa yhteyttä, valittiin internetistä saatujen tietojen perusteella.

Haastateltavaksi haluttiin erikokoisia SaaS-organisaatioita, jota voidaan kutsua laajan vaihtelun otannaksi, koska kohteeksi haettiin ns. toisistaan poikkeavan kokoisia organisaatioita (Liamputtong ja Ezzy 2007, 46). Lopulta haastateltavat organisaatiot valikoituivat vapaaehtoisuuden periaatteella (Liamputtong ja Ezzy 2007, 48) eli haastateltiin vain tutkimukseen suostuneita organisaatioita. Tutkimuksen laajan vaihtelun otanta ei aivan toteutunut, sillä suurin osa tutkittavista organisaatioista oli lähes saman kokoisia, mutta kaikkiaan organisaatioiden kokovaihtelu toteutui, sillä yritysten henkilöstömäärä oli aina 12 henkilöstä 6700 henkilöön. Alun perin tarkoitus oli haastatella viestinnän ammattilaisia, mutta koska osassa haastateltavaksi suostuneissa organisaatioissa viestinnästä vastasi toimitusjohtaja tai joku muu henkilö, ja lisäksi muutamasta organisaatiossa haluttiin haastateltavan toimitusjohtajaa, viestinnänammattilaisen sijaan, olivat haastateltavat pääsääntöisesti oman työn ohessa viestintää tekeviä toimitusjohtajia. Vain yksi haastateltava oli kokopäiväinen viestintäpäällikkö. Ymmärrettävästi toimitusjohtajien ajankäyttö viestintään oli vähäistä, mutta kuten taulukosta neljä nähdään, silti haastateltava kolme ja kuusi käyttävät lähes puolet työajastaan viestintään.

Tutkittavien määrä ei laadullisessa tutkimuksessa ole tärkeintä, koska tarkoitus ei ole yleistää saatavia tutkimustuloksia vaan kuvata nykytilannetta (Tuomi ja Sarajärvi 2002, 87). Tässä tutkimuksessa lopullinen haastateltavien määrä oli kahdeksan henkilöä. Koska haastateltavia on vähän, ovat Tuomi ja Sarjajärvi (2002, 88) sitä mieltä, että haastateltavien valinta tulee tehdä sen mukaan, että heiltä saisi mahdollisimman hyvin tietoa tutkittavaan aiheeseen. Tästä syystä haastateltavaksi valittiin organisaation viestinnästä vastuussa olevia henkilöitä. Haastateltavien tärkeimmät taustatiedot on koottu taulukkoon 4.

TAULUKKO 4. Haastateltavien taustatietoja.

haastateltava	**titteli**	**viestintä kokopäivätyötä vai työn ohessa**	**ajankäyttö viestintään**	**henkilöstö-määrä**
haastateltava 1	tj	ohessa	pieni	50-200
haastateltava 2	tj	ohessa	5%	alle 50
haastateltava 3	tj	ohessa	40%	alle 50
haastateltava 4	vp	kokopäivätyö	100%	yli 200
haastateltava 5	sj	ohessa	20%	50-200
haastateltava 6	tj	ohessa	30-50%	50-200
haastateltava 7	tj	ohessa	10%	alle 50
haastateltava 8	tj	ohessa	15%	50-200

3.3 Haastattelu aineiston keruumenetelmänä

Tutkimusaineiston hankintamuodoksi valittiin haastattelu, sillä se on laadullisen aineiston keruumenetelmänä joustava, ja se soveltuu aiheisiin, joita voidaan pitää vaikeina. Lisäksi haastattelun aikana voidaan oikaista mahdollisia väärinkäsityksiä, selventää kysymyksiä,

pyytää tarkennuksia sekä esittää tarvittaessa haastateltavalle jatkokysymyksiä (Tuomi ja Sarajärvi 2002, 74, 35-36.) Tutkimus kyberturvallisuusuhkiin ja -ympäristöön liittyen ajateltiin aiheeltaan sellaiseksi, että haastattelu on paras tiedonkeruumenetelmä, koska aihe ei ole viestintää tekeville tai muillekaan välttämättä tuttu ja haastattelun aikana olisi mahdollista tehdä tarkennuksia ja selvennyksiä puolin ja toisin.

Haastattelumuodoksi valittiin puolestaan teemahaastattelu, joka tarkoittaa, että haastattelussa keskitytään yhteen tai muutamaan teemaan eli tutkittaviin liittyviin asioihin (Alasuutari 2011, 51). Teemahaastattelu tarkoittaa myös sitä, että kaikille haastateltaville esitetään samat kysymykset ja teemat on päätetty etukäteen. Haastattelussa tulee esille haastateltavan omat tulkinnat teemoista (Hirsjärvi ja Hurme 2000, 47- 48, 66.) Tässä tutkimuksessa keskityttiin teemoihin: luotettavuus, kyberturvallisuusuhkat ja sidosryhmäverkostot.

Haastattelututkimus toteutettiin puhelinhaastatteluna 26.2. – 15.3.2018 välisenä aikana. Puhelinhaastattelu on kustannustehokas ja joustava haastattelumuoto. Sen avulla voi olla myös esimerkiksi paras tapa tavoittaa tietyt ihmiset (Ikonen 2017, 270-273, 274-285, 280). Menetelmä osoittautui tässä tutkimuksessa toimivaksi, sillä osa haastateltavista suostui tutkimukseen vain siksi, että haastattelu suoritettiin puhelimitse. Lisäksi tutkimuksen toteutuksen aikataulu oli tiukka. Yleensä haastattelun etuna pidetään ei-kielellisiä vihjeitä, jotka antavat vastausten lisäksi lisätietoja (Hirsjärvi ja Hurme 2000, 34), mutta puhelinhaastattelussa kaikkia sävyjä ei saada havainnoitua ja tallennettua (Ikonen 2017, 270-273). Tässä tutkimuksessa se ei ollut ongelma, koska pääasia oli haastateltavan vastauksien sisällöllä, ei käyttäytymisellä tai sanattomilla vihjeillä.

Ennen puhelinhaastattelua suositellaan ottamaan yhteyttä haastateltavaan joko kirjeitse ja puhelimitse tai sekä että. Viimeistään haastatteluajankohta on hyvä sopia puhelimitse, jolloin tutkijalle voi myös esittää kysymyksiä haastattelusta ja tutkimuksesta (Hirsjärvi ja Hurme, 2000, 64). Ikonen (2017, 279) pitää myös tärkeänä, että yhteydenotto tehdään huolellisesti valmistautuneena ja kerrotaan omasta tutkimuksesta ja sen tavoitteista. Haastateltavaksi haluttuihin SaaS-organisaatioihin otettiin yhteyttä puhelimitse ja soittoja tehtiin yhteensä 12 organisaatioon, joista lopullisesti haastatteluun suostui kahdeksan organisaatiota. Kontaktipuhelun pohjana käytettiin samaa pitchaus- eli markkinointikirjettä (liite 1), joka lähetettiin haastattelua harkitseville ja siihen jo lupautuneille. Kontaktipuheluiden jälkeen markkinointikirje lähetettiin sähköpostitse, mutta sitä muokattiin erilaiseksi haastattelua harkinneille ja jo haastatteluun lupautuneille. Niille, jotka tekivät päätöksen haastatteluun osallistumisesta markkinointikirjeeseen tutustumisen jälkeen, haastatteluaika sovittiin sähköpostitse ja muiden kanssa aika sovittiin kontaktipuhelun yhteydessä.

Haastattelun avulla on mahdollisuus saada paljon tietoa ja jotta tietoa saisi tutkimusaiheeseen mahdollisimman tarkasti, pitävät Tuomi ja Sarajärvi (2002, 75) tärkeänä, että haastateltava saa kysymykset tai aiheen etukäteen valmistautuakseen haastatteluun. Tässä tutkimuksessa haastatteluun valmistautumisen voidaan nähdä alkaneen ensimmäisestä puhelinsoitosta, jolloin kerrottiin tutkimusaiheesta. Lisäksi – kuten edellä mainittiin, haastateltaville lähetettiin myös sähköpostitse lisätietoa markkinointikirjeellä (liite 1). Haastateltavilla oli myös mahdollisuus ottaa yhteyttä mahdollisten lisätietojen saamiseksi. Ennen haastattelua tutkimuksen ja haastattelun aihe vielä kerrattiin haastateltavalle ja kysyttiin, oliko haastateltavalle herännyt kysyttävää aiheeseen tai haastatteluun liittyen.

Kysymysten määrän suhteen Williamson ja Bow (2002) suosittelevat olemaan tarkkana, ettei kysymyksiä olisi liikaa ja että ne koskisivat tarkasti omaa tutkimusaihetta. Liial-

linen kysymysten määrä tekee haastattelusta raskaan ja liian laveat kysymykset eivät lopulta merkityksellistä aineistoa. (Williamson ja Bow, 2002, 92.) Tässä tutkimuksessa kysymykset testattiin kahdella henkilöllä, jotta nähtiin, kuinka kysymykset ymmärretään ja kauanko haastatteluun menee aikaa. Testihaastattelujen jälkeen kysymyksiä hiukan muokattiin ja saatiin lopullinen haastattelurunko (liite 2). Haastattelurunko sisälsi kaikkiaan 22 kysymystä, joista taustakysymyksiä oli kuusi, varsinaisia tutkimuskysymyksiä 13 ja muita kysymyksiä kolme. Käytännössä kysymysten määrä oli toimiva ja haastateltavat jaksoivat vastata kysymyksiin hyvin.

Haastattelun keskeinen piirre on keskustelunomaisuus (Hirsjärvi ja Hurme 2002, 103; Liamputtong ja Ezzy 2007, 55). Keskustelunomaisuuteen pyrittiin tutkimuksessa esittämällä kysymykset puhekielellä ja mm. viittaamalla haastatellun aikaisempiin vastauksiin ja kommentoimalla haastateltavan sanomaa esimerkiksi, ”aivan”, ”joo”, ”kyllä” -kommenteilla. Aikarajan ja kysymysten määrän vuoksi tämän luontevampaan keskusteluun ei kuitenkaan ollut mahdollisuutta. Puhelinhaastattelun maksimikestona pidetään 20-30 minuuttia (Hirsjärvi ja Hurme 2002, 64) ja osalle haastateltavia olikin merkitystä, ettei haastattelu kestäisi pidempään. Tässä tutkimuksessa haastattelut kestivät 24 -30 minuuttia.

Nauhurille tallentamista pidetään hyvänä keinona keskittyä haastateltavan sanomiseen, koska silloin ei tarvitse tehdä muistiinpanoja ja koska nauhoitetusta puheesta saadaan kerättyä enemmän tietoa (Liamputtong ja Ezzy 2007, 67). Menetelmä koettiin hyväksi myös tässä tutkimuksessa. Puhelinhaastattelut nauhoitettiin erilliselle nauhurille ja tallennettiin sen jälkeen koneelle jatkokäsittelyä varten.

3.4 Tutkimusaineiston analysointi

Tutkimusaineiston analysointimenetelmäksi valittiin laadullinen analyysi, joka tarkoittaa ”aineiston käsittelemistä usein kokonaisuutena” (Alasuutari 2011, 38). Laadullisen analyysin ja ylipäätään laadullisen tutkimuksen luotettavuus tulee varmistaa ja yksi tapa varmistaa luotettavuus on kertoa, minkä seurauksena on tultu kyseisiin johtopäätöksiin (Tuomi ja Sarajärvi 2002, 138).

Tämän tutkimuksen kohdalla voidaan myös puhua laadullisesta aineistolähtöisestä sisällönanalyysistä, joka alkaa haastattelujen kuuntelemisella (Tuomi ja Sarajärvi 2002, 111) ja sen jälkeen litteroimisella. Tarkkuus litteroinnissa määrittyy tutkimuskysymysten (niihin saadaan vastaus) ja analyysitavan perusteella (Ruusuvuori ja Nikander 2017, 427). Koska tässä tutkimuksessa ei ollut merkitystä ilmaisutavalla tai tilkesanoilla (esim. huokauksilla tai ”tota niinku” -ilmaisuilla), litteroitiin haastatteluista vain asiasisältö.

Empiiriseen ja laadulliseen tutkimukseen kuuluu mm., että tutkittavien tunnistettavuus poistetaan (Tuomi ja Sarajärvi 2002, 21). Anonymisointi eli tunnistettavien tietojen, esimerkiksi nimien ja organisaatiotietojen poisto tehdään litterointivaiheessa ja haastateltavat voidaan koodata numeroilla (Swanson ja Holton 2005, 240). Tässä tutkimuksessa haastateltavia oli vähän, joten heidät laitettiin numeeriseen järjestykseen haastatteluiden mukaisesti.

Tutkimukseen osallistuvien ei saa myöskään joutua kokemaan minkäänlaista harmia tai vahinkoa ja heidän tulee pystyä luottamaan siihen, että tutkimusaineistoa käytetään vain kyseiseen tutkimukseen, eikä tietoja luovuteta ulkopuolisille. (Tuomi ja Sarajärvi 2002, 128-

129.) Tässä tutkimuksessa aineiston säilyttämisestä ja hävittämisestä kerrottiin ensimmäisen puhelinsoiton aikana, siitä kerrottiin markkinointikirjeessä ja asia kerrattiin vielä haastattelun yhteydessä.

Litteroinnin jälkeen aineisto pelkistettiin eli redusoitiin. Tällöin käsiteltäväksi jätetään vain tutkimuksen kannalta olennainen tieto, joka tapahtuu siten, että haastatteluaineistosta haetaan tutkimukseen liittyviä käsitteitä ja ilmaisuja ja suorat ilmaukset pelkistetään. (Tuomi ja Sarajärvi 2002, 110-111.) Tässä tutkimuksessa tämä tarkoitti esimerkiksi sitä, että haastateltavien vastauksista haettiin sanoja ja ilmaisuja, joilla haastateltavat kuvailivat luotettavuutta, kyberturvallisuusuhkia ja digitaalisia sidosryhmäverkostoja.

Pelkistämisen jälkeen tehtiin puolestaan klusterointi. Tässä vaiheessa aineistosta haetaan käsitteistä yhtäläisyyksiä ja eroja ja ne ryhmitellään omiksi luokiksi. Voidaan puhua myös teemoittelusta, joka tarkoittaa, että aineistosta haetaan ”*nousevia piirteitä, jotka ovat yhteisiä usealle haastateltavalle*.” (Hirsjärvi ja Hurme 2000, 173). Ne voivat pohjautua haastattelun teemoihin (Hirsjärvi ja Hurme 2000, 173), kuten oli tässä tutkimuksessa (luotettavuus, kyberturvallisuusuhkat ja toimijaverkostot).

Abstrahointi eli käsitteellistäminen tarkoittaa, että aineiston analysointi viedään vielä käsitteellisemmälle tasolle (Tuomi ja Sarajärvi 2002, 112-115) ja yhdistetään tuloksiin teoriat ja aiemmat tutkimukset (Eskola 2015, 198, 201.) Tämä vaihe on luettavissa kappaleesta johtopäätökset.

4 TULOKSET

Haastatteluista saadut tulokset esitetään tutkimuksen teemojen mukaisesti seuraavassa järjestyksessä: luotettavuus, kyberturvallisuusuhkat ja digitaaliset sidosryhmäverkostot. Haastattelurunko löytyy kokonaisuudessaan liitteistä (LIITE 2).

4.1 Luotettavuus digitaalisissa sidosryhmäverkostoissa

Luotettavuutta selvitettiin seitsemällä kysymyksellä, joiden tarkoituksena oli selvittää, miten organisaatioissa määritellään luotettavuutta ja miten se tulee esille viestinnässä kyberympäristössä.

Ensin haastateltavilta kysyttiin, miten kunkin mielestä oma organisaatio on luotettava ja miten se tulee esille. Näiden jälkeen kysyttiin, miten haastateltavan mielestä oma organisaatio tuo viestinnässä esille olevansa rehellinen, tasapuolinen, oikeudenmukainen, lakeja ja säädöksiä noudattava, asiakkaille lisäarvoa tuottava, asiantuntija ja turvallinen yhteistyökumppani digitaalisissa sidosryhmäverkostoissa. Kaikki nämä kysymyksissä olleet käsitteet ovat kirjallisuudessa esiin tulleita määreitä luotettavuudelle.

4.1.1 Luotettavuus ja viestintä

Organisaation luotettavuutta ja siitä viestimistä kysyttiin haastateltavilta kysymyksillä (kysymykset yhdeksän ja kymmenen): miten kuvailisit organisaation luotettavuutta digitaalisissa sidosryhmäverkostoissa ja mitkä viestinnälliset tekijät mielestäsi vaikuttavat siihen, että organisaatio koetaan luotettavaksi digitaalisissa sidosryhmäverkostoissa.

Viestinnällisesti luotettavuutta kuvattiin eniten asiantuntijuudella. Eli luotettavuus näkyy viestinnän sisällössä esimerkiksi organisaation omien asiantuntijoiden kirjoituksina mm. blogeissa ja osallistumisena sosiaalisen median keskusteluihin ja asiakkaiden auttamisena. Lisäksi asiantuntijat verkostoituivat organisaation ulkopuolisten asiantuntijoiden kanssa ja loivat yhdessä sisältöä eri keinoin ja eri kanavissa.

> *”…rakennetaan sitä kautta luottamusta, kun tuodaan asiantuntijuutta esiin, pystytään antamaan vinkkejä yrityksille, miten he pystyvät hoitamaan asioita paremmin ja tehokkaammin…”*

Usean vastaajan mielestä viestintä loi luotettavuutta, kun se on ammattimaista, henkilöt ovat tunnistettavissa ja käytössä ovat useat eri kanavat. Myös viestinnän avoimuudella ja rehellisyydellä sekä luottamuksellisuudella nähtiin olevan vaikutusta organisaation luotettavuuteen.

> *" …aito rehellisyys, uskalletaan kertoa niin hyvistä, ku huonoista asioista, ehkä myös sellanen tietynlainen maanläheisyys…meillä on hyvin maanläheinen ote ja, sit ollaan avoimia omista asioista, mutta muiden ihmisten asiat pidetään luottamuksellisina…rehellisyys ja maanläheisyys on ne kulmakivet, et ois se mielikuva, että ois luotettava."*

Osa haastateltavista oli sitä mieltä, että mm. organisaation historia (esim. yrityksen toiminnan selaaminen verkossa) ja tunnettuus vaikuttavat siihen, että se koetaan luotettavaksi.

> *"…meitä pidetään luotettavana jo meidän historiankin vuoksi, eli on 15 vuotta vanha yritys…"*

> *"…se, että meillä on paljon tunnettuja asiakkaita, jotka on meidän kumppanina ja ostanu meidän tuotetta…"*

Muutama vastaaja ei kuitenkaan uskonut, että organisaatio itse voi vaikuttaa suoraan sen luotettavuuteen vaan referenssit ja oman työn jälki luovat ensisijaisesti luotettavuutta.

> *"Mä uskon, ettei siihen itse voi niin paljon vaikuttaa suoraan, vaan mitä muut puhuvat meistä tai se, että miten hyvin me hoidetaan meidän asiakkaita, niin asiakkaat puhuu meistä hyvää sitten muille. Ja siitä syntyy luotettu maine."*

Poikkeavin vastaus oli, kun eräs haastateltava piti sovelluskaupan latausmääriä luotettavuuden tekijänä.

Organisaation luotettavuutta kuvattiin useilla erilaisilla positiivisilla ilmaisuilla. Moni haastateltava kuvaili organisaationsa luotettavuutta sanalla luotettava. Muita ilmaisuja olivat vastuuntuntoinen, arvostettu, rehellinen, maanläheinen, tunnettu, innovatiivinen, moderni ja dynaaminen.

4.2 Rehellisyys, tasapuolisuus ja oikeudenmukaisuus viestinnässä

Seuraavaksi kysyttiin (kysymys 11), millä tavalla vastaajan mielestä oma organisaatio tuo esille olevansa rehellinen, tasapuolinen ja oikeudenmukainen digitaalisissa sidosryhmäverkostoissa.

Viestinnän avoimuus oli suurimman osan mielestä tekijä, jolla organisaation rehellisyys tulee esille. Esimerkiksi eräs organisaatio kertoi yrityksen asioista enemmän mitä lait ja säädökset vaativat, jossakin vastaavasti tuotiin avoimesti esille organisaation epäonnistumiset tai epätäydellisyys.

"…kirjotetaan vaikka juttuja, niin laitetaan, mitä on opittu matkan varrella, että ei olla kaikkien asioiden asiantuntijoita…ja laitetaan sinne vähän, mitä oltas voitu tehdä toisin…"

Eräs organisaatio toi puolestaan esille teknologiansa rajallisuuden, mutta kertoi myös sen mahdollisuuksista. Avoimuus ilmeni myös ikävien päätösten perustelemisena.

" viestitään omissa nimissä, ikävätkin asiat kerrotaan ja pyritään sitte myös aina perustelemaan asioita, esim. miksi jouduttiin nostamaan hintoja…"

Digitaalisessa ympäristössä rehellisyytenä ja avoimuutena viestinnässä pidettiin myös henkilöstön tunnistettavuutta. Muutaman haastateltavan mielestä avoimuus ja rehellisyys ilmenivät lisäksi viestimällä asiakastarinoita ja -kokemuksia, avun antamisena ja sisällön monipuolisuutena. Muutama haastateltava mainitsi myös vastuullisuuden esilletuomisen viestinnässä. Erään haastateltavan mielestä rehellisyys ja avoimuus näkyivät luottamuksellisuutena eli kerrottiin vain se, mitä oli asiakkaan kanssa sovittu ja, että organisaation teot olivat mitattavissa. Joku oli taas sitä mieltä, että heidän tuote loi rehellisyyttä ja luottamusta.

"meidän tuote on semmoinen niinku osallistamisen ja organisaatioitten kestävän muutoksen platformi, jolloin koko viestintä perustuu ideologiaan, että yhdessä tekeminen ja johdettu osallistava muutos on keskeinen hyöty…"

Tasapuolisuutta ja oikeudenmukaisuutta kuvailtiin vastauksissa erityisesti kumppanuutena ja tasavertaisuutena asiakkaiden kanssa.

Usea vastaaja oli kuitenkin sitä mieltä, että niin tasapuolisuus, oikeudenmukaisuus kuin rehellisyyskin tulevat esille enemmän epäsuorasti. Esimerkiksi ne voivat olla integroituina kaikkeen - organisaation kulttuuriin ja tapaan toimia.

"…ei välttämättä viestitä erikseen sen tyyppisistä teemoista, mutta sitä tavallaan tuodaan esiin erinäisissä yhteyksissä…"

Epäsuorasti rehellisyys, tasapuolisuus ja oikeudenmukaisuus tulivat vastaajien mielestä esille myös asiakkaiden kautta mm. referensseinä ja asiakastarinoiden kautta.

"Kyl se meidän maine ei synny suorilla viestinnän teoilla vaan enemminkin, miten me toimitaan suhteessa asiakkaisiin ja hoidetaan niitä asiakkaita…Sitä kautta syntyy luotettu maine."

4.2.1 Lakien ja sääntöjen noudattaminen viestinnässä

Lakien ja sääntöjen noudattamisen näkymistä viestinnässä kysyttiin, miten oma organisaatio tuo digitaalisissa sidosryhmäverkostoissa viestinnällä esille noudattavansa lakeja ja muita sääntöjä (kysymys 12). Vastaajien mielestä asia ilmeni erityisesti viestinnän sisällöissä, joissa korostettiin suoraan tai epäsuorasti organisaation asiantuntijuutta, esimerkiksi yhtä haastateltavaa lukuun ottamatta organisaatioissa oli tuotu esille omaa tietämystä ja valveutuneisuutta GDPR:stä.

GDPR-uudistus liittyy Suomen tietosuojalain ja Euroopan unionin tietosuoja-asetuksen uudistumiseen ja yhtenäistämiseen toukokuussa 2018. Lyhyesti sanottuna muutos koskee henkilötietoja koskevien tietojen keräämistä, päivittämistä, käsittelyä ja säilyttämistä. Henkilötietojen käsittelystä on tehtävä suunnitelmat ja ne on dokumentoitava. Mitä riskialttiimpia henkilötietoja käsitellään, sitä suuremmat velvollisuuden rekisterin pitäjällä on. Lain ja tai asetuksen rikkomisesta on seurauksena sanktio tai henkilötietojen käsittelykielto. (Suomen tietosuojavaltuutetun verkkosivut.) SaaS-organisaatioita uudistus koskee sekä asiakkaiden että yritysten oman toiminnan kautta. Useissa organisaatioissa asiakkaat voivat käsitellä henkilötietoja SaaS-palveluita käyttäessään ja lisäksi moni SaaS-palveluja tarjoava organisaatio käsittelee henkilötietoja oman organisaationsa sisällä.

Lisäksi sidosryhmille kerrottiin mm. organisaation erityisosaamisesta ja henkilöistä niiden takana ja miten organisaatio on perillä muistakin alan muutoksista ja niihin varautumisesta. Sisällössä korostui asiantuntijuuden lisäksi asiakkaiden auttaminen.

> *"…tuodaan esille, että me ollaan perillä näistä muutoksista ja miten meidän asiakkaiden tulisi ottaa ne huomioon omassa liiketoiminnassaan…tuodaan esiin, että me ollaan kiinnostuttu, ei pelkästään omalta kantilta, mut me ollaan myös auttamassa asiakkaita vastaamaan näihin muutoksiin ja uusiin vaatimuksiin."*

Viestinnän sisällön suhteen pidettiin myös tärkeänä, että se oli ymmärrettävää. Eräs haastateltava sanoikin, että lakeihin liittyvää viestintää pyritään yksinkertaistamaan, jotta muutkin kuin asian ammattilaiset ymmärtäisivät sen. Tuotetun sisällön ei tarvinnut olla myöskään omaan palveluun liittyvää, vaan sisältöä ja aineistoa tehtiin epäsuorasti omaan toimintaan liittyen ja laajemmin kuin vain omille asiakkaille.

> *"…tuotettu blogiposteja ja asiakasmateriaalia, jota voivat käyttää omassa työssään, vaikka eivät olisi meidän asiakkaita."*

> *"…pyritään kirjottamaan näistä aiheista, miten esim. gdpr vaikuttaa meidän asiakaskuntaan tai sen tyyppisiin ihmisiin, jotka vois olla meidän asiakaskuntaa…"*

Lakien ja sääntöjen noudattamisesta kertoi muutaman vastaajan mielestä myös se, että organisaatio kertoi saamistaan erilaisista sertifikaateista, toi esille sopimuksia tai sopimuspohjia ja listasi ohjeistuksia. Sertifikaateista kertominen oli erään vastaajan mielestä myös tapa yksinkertaistaa viestintää ymmärrettävämmäksi.

> *"sertifikaateilla ja muilla on pyritty yksinkertaistaa sitä viestiä…"*

Haastateltavien vastauksissa tuli viestinnän sisällön ja ymmärrettävyyden lisäksi esille viestinnän eri kanavat ja keinot. Kanavissa korostui sosiaalisen median kanavat ja yrityksen verkkosivut. Keinoina mainittiin vastaavasti blogit, uutiskirjeet, asiakasmateriaalit, ja myyntimateriaalit.

> *"Meillä on oma blogi verkkosivustolla…konserniyhtiöillä on omia nettisivuja…konsernisivulle luodaan omaa nettisivupohjaa vielä erikseen.. jaetaan materiaaleja sosiaalisen median kanavissa ja asiakaskanavassa."*

Lisäksi osa järjesti seminaareja internetyhteydellä tai webinaareja, joissa annettiin lisätietoa tai koulutettiin asiakkaita tai eri sidosryhmiä laeista ja säädöksistä.

Jotkut eivät kuitenkaan nähneet lakien ja säädösten viestimistä lainkaan tärkeänä.

"Ei siitä tarvitse erikseen viestiä, kun lähtökohta on, että lakeja noudatetaan."

4.2.2 Lisäarvon tuottaminen

Haastateltavan organisaation lisäarvon tuottamista digitaalisissa sidosryhmäverkostoissa selvitettiin kysymyksellä 13.

Lisäarvoa tuotettiin vastaajien mielestä eniten asiantuntijasisällöllä. Se tuli esille mm. omien ja ulkopuolisten asiantuntijoiden sekä muiden sidosryhmäläisten kirjoittamina asiantuntijapuheenvuoroina.

"…meidän omien asiantuntijoiden puheenvuoroja, esim. mitä saa työkalusta irti…asiakkaitten tarinoita…julkaistaan tämmösessä sarjassa ulkopuolisen, joka voi olla asiakas, verkostolainen tai muuten vaan ansioitunut tällä toimialalla, kirjotuksia…"

"…tavallaan me ei kerrota suoraan, kuinka hyviä ollaan, vaan tuodaan nimenomaan asiantuntemusta esille substanssilla, kiinnostavaa sisältöä asiakkaille…"

Asiantuntijuuden lisäksi tärkeänä pidettiin viestinnän sidosryhmälähtöisyyttä. Yhtä vastaajaa lukuun ottamatta viestinnän sisällön hyödyllisyys ja kiinnostavuus olivat tapoja tuoda lisäarvoa sidosryhmille ja / asiakkaille. Organisaatiot halusivat auttaa ja lisätä asiakkaiden osaamista: helpottaa arkea, opastaa, antaa vinkkejä ja lisätä yleistä tietämystä. Aina annetun tiedon ei tarvinnut liittyä omaan tuotteeseen.

"Meillä tulee esimerkiksi joka viikko ilmainen video, missä on vinkkejä, eikä sinällään liity meidän tuotteeseen millään lailla…yleisesti pyritään sidosryhmiä auttamaan, että olis enemmän tietoa…"

Vaikka osassa vastauksissa korostui yleinen sidosryhmien auttaminen, osa koki lisäarvon tuottamisen nimenomaan asiakkaille suunnattuna asiana. Esimerkiksi asiakkaille oli erikseen tuotettua lisämateriaalia ja erilaisia yhteistyökuvioita sekä asiakkaiden näkyvyyttä pyrittiin parantamaan omien viestintäkanavien kautta. Eräässä organisaatiossa oli myös asiakkaille oma tukiportaali, jossa heille jaettiin mm. syvällisempää tietoa ostamastaan palvelun käytöstä.

Lisäarvon tuottamisena pidettiin myös tiedon vaivatonta saatavuutta ja viestien ymmärrettävyyttä.

"…tavallaan yritetään saada sitä asiantuntijuutta tuotua alaspäin, että puhutaan mahdollisimman ruohonjuuritason asiasta, mitä sitten vois noudattaa omassa arjessa…"

Useat haastateltavat pitivät myös monipuolisia viestinnän keinoja tapana tuottaa lisäarvoa. Esimerkkinä mainittiin tukiportaalin lisäksi ekirjat/ ebookit, blogikirjoitukset, videot ja webinaarit. Blogin maininnut haastateltava oli myös sitä mieltä, että useiden keinojen ja

kanavien lisäksi lisäarvoa tuotettiin viestinnän jatkuvuudella. Esimerkiksi blogeja kirjoitettiin säännöllisesti kerran viikossa ja useita e-kirjoja oli julkaistu muutaman kuukauden sisällä.

4.2.3 Asiantuntijuuden ja osaamisen viestiminen

Asiantuntijuutta sivuttiin jo aiemmissa vastauksissa, mutta varsinaisesti siitä kysyttiin kysymyksellä 14: millä tavalla organisaatio tuo viestinnällä esille omaa asiantuntijuutta ja osaamista digitaalisissa sidosryhmäverkostoissa. Koska haastateltavat olivat maininneet asiasta jo aiemmissa vastauksissaan, oli ymmärrettävää, että osan vastaukset olivat joltain osin aiemman toistoa.

Asiantuntijuus ja osaaminen tuli viestinnässä esille joidenkin vastaajien mielestä muun muassa siten, että viestintää tekevät olivat tunnistettavissa sosiaalisessa mediassa esimerkiksi omilla nimillään ja kasvoillaan ja tekijöitä oli useita sekä tieto oli helposti saatavilla.

Viestinnän sisältö ja sen sidosryhmälähtöisyys olivat myös vastauksissa tärkeässä roolissa. Vastausten perusteella haastateltavat pitivät tärkeänä sisällön relevanttiutta ja auttamista sekä sidosryhmien yleisen tietämyksen lisäämistä.

> *"…että saisivat tiedon helposti, saavat apuja kaikkeen semmoseen myös, mikä ei suoranaisesti liity meidän ohjelmistoihin ja järjestelmiin, eikä siihen asiakkuuteenkaan vaan kun tulee näitä kaikkia koskevia muutoksia tai meillä on vinkkejä jakaa…meillä on parhaita käytäntöjä ja jaetaan niitä, niin tarkotus on aina helpottaa asiakkaan liiketoimintaa ja sujuvoittaa elämää, että tuotas sellasta hyödyllistä sisältöä omissa kanavissamme esiin…"*

Eräs haastateltava mainitsi erikseen, että heidän organisaatiossa oli tehty viestintään sisältöstrategia.

Muutama haastateltava piti jälleen tärkeänä myös viestinnän ymmärrettävyyttä ja yhdessä organisaatiossa asiantuntijaviestinnän parantamiseksi haettiin apua talon ulkopuolelta.

> *"…he saavat ulkopuolelta ostettua tukea siihen, miten kannattaa asioita ilmaista ja miten sen teeman saa esimerkiksi rakennettua mahollisimman selkeeksi…että se peruskäyttäjä, joka tuolla on, niin ei ymmärrä sitä kyllä tuolla tasolla, niin siihen tarvitsee tosi paljon tukea…"*

Esille tulivat myös vahvasti erilaiset viestinnän keinot, joilla asiantuntijuutta ja osaamista tuotiin esille.

> *"…tuotetaan sisältöä, jotka voi olla blogeja tai e-kirjoja, oppaita, webinaareja ja videoita tehdään, järjestetään tapahtumia, jotka streemataan esim. Facebookiin ja muualle…"*

> *"…webbisivuilla on aika paljon sellasta asiantuntijasisältöä, sit me järjestetään webinaareeja, on erilaisia kasvokkaistapaamisia, osallistutaan alan eri tapahtumiin, julkaistaan uutiskirjeitä, ja sitten tää blogimaailma on olennaisessa roolissa ja siihen liittyvä sosiaalisen median käyttö…"*

Muutaman haastateltavan mielestä he eivät tuo viestinnässä esille asiantuntijuutta ja osaamista digitaalisissa sidosryhmäverkostoissa.

"No se on varmastiki semmonen asia, että se on lapsipuolen asemassa digitaalisessa ympäristössä…ei tuoda sitä erikseen nostaen"

On kuitenkin huomioitava, että samainen haastateltava sanoi muun vastauksen yhteydessä, että organisaatio viestii teknologiasta.

Lisäksi merkille pantavaa oli, että vain yksi haastateltava kertoi, että heillä asiantuntijuuden esilletuomisen keinoina käytettiin myös yhteiskunnallista vaikuttamista ja monitorointia.

"Me otetaan kantaa erilaisiin yhteiskunnallisiinkin asioihin ja tavallaan tuodaan ratkaisuja ongelmiin ja haasteisiin, mitä huomataan että asiakkailla on tai mitä on keskusteluissa yhteiskunnallisestikin…me tuodaan esiin meidän oma kanta ja ratkaisuehdotuksemme ja vinkkimme….me ei tuoda sitä välttämättä esiin ohjelmistokärjellä vaan keskustellaan enemmän siitä, että….esimerkiksi, miten tuo säästöä ja tehostaa toimintaa, miten parantaa työntekijätyytyväisyyttä ja asiakaspalvelua…"

4.2.4 Viestintätavat turvallisen yhteistyön kokemiseen

Viimeisessä varsinaisessa luotettavuutta käsittelevässä kysymyksessä selvitettiin, millä viestinnän tavoilla oma organisaatio haastateltavan mielestä vaikuttaa siihen, että yhteistyö sen kanssa koetaan turvalliseksi digitaalisissa sidosryhmäverkostoissa. Eniten turvallisuutta pyrittiin rakentamaan ihmisten eli henkilöstön ja ihmisten tunnistettavuuden avulla.

"…ihmiset esiintyy omilla nimillä, omilla kasvoilla eli meillä viestintä ei ole vain yrityksen omissa nimissä tapahtuvaa viestintää, meidän kaikki henkilöt on omilla nimillä jakamassa, osallistumalla näihin keskusteluihin…"

Tunnistettavuuteen liittyi myös työntekijöiden todellisen olemassaolon todistaminen ja siksi eräässä organisaatioissa pidettiin mm. onlinepalavereita /-kokouksia ulkoisten asiakkaiden kanssa. Tämän lisäksi muuan haastateltava kertoi, että heillä korostettiin työntekijöiden mukavuutta ja helposti lähestyttävyyttä.

Turvallisuutta luotiin myös viestimällä erilaisista sopimuksista ja sertifikaateista, jotka tulivat esille haastateltavilta jo lakien ja normien noudattamista kysyttäessä. Osalla oli myös keinoina kolmannen osapuolen auditoinnit ja tekniset materiaalit. Osassa organisaatioita näissä pyrittiin huomioimaan sidosryhmälähtöisyys ja niitä tuotiin esille mm. organisaation verkkosivuilla.

"…et on näitä materiaaleja ja pyritään, että ovat asianmukaisia ja käyttäjäystävällisiä."

Eräässä haastateltavan organisaatiossa oli käytössä CSM eli customer success management -prosessi, jolla uskottiin myös olevan vaikutusta siihen, miksi yhteistyö voidaan kokea turvalliseksi.

Muutamassa vastauksessa nousi esille viestinnän avoimuus, sillä eräs haastateltava piti tärkeänä, että heillä kerrotaan organisaation toiminnasta ja kulttuurista, toinen taas oli sitä mieltä, että kun kerrotaan mahdollisimman selkeästi, mitä he tekevät ja mitä eivät tee, niin se luo turvallisuutta. Joku näki vastaavasti turvallisuuden luomisena sen, että heillä

asiakkaille kerrotaan konsernin pienten yhtiöiden asiakasläheisyydestä ja ketteryydestä, mutta toisaalta tuodaan esille, että tukena on myös iso konsernitason koneisto.

Yhteistyön turvallisuutta luotiin myös viestimällä asiakkaista. Esimerkiksi kerrottiin asiakastarinoita ja tuotiin esille asiakasreferenssejä sekä yhteistyötä asiakkaiden kanssa.

> *"…et kysellään asiakkailta…ja otetaan asiakkaita mukaan tapahtumiin…asiakkaan aito ääni tulee esille."*

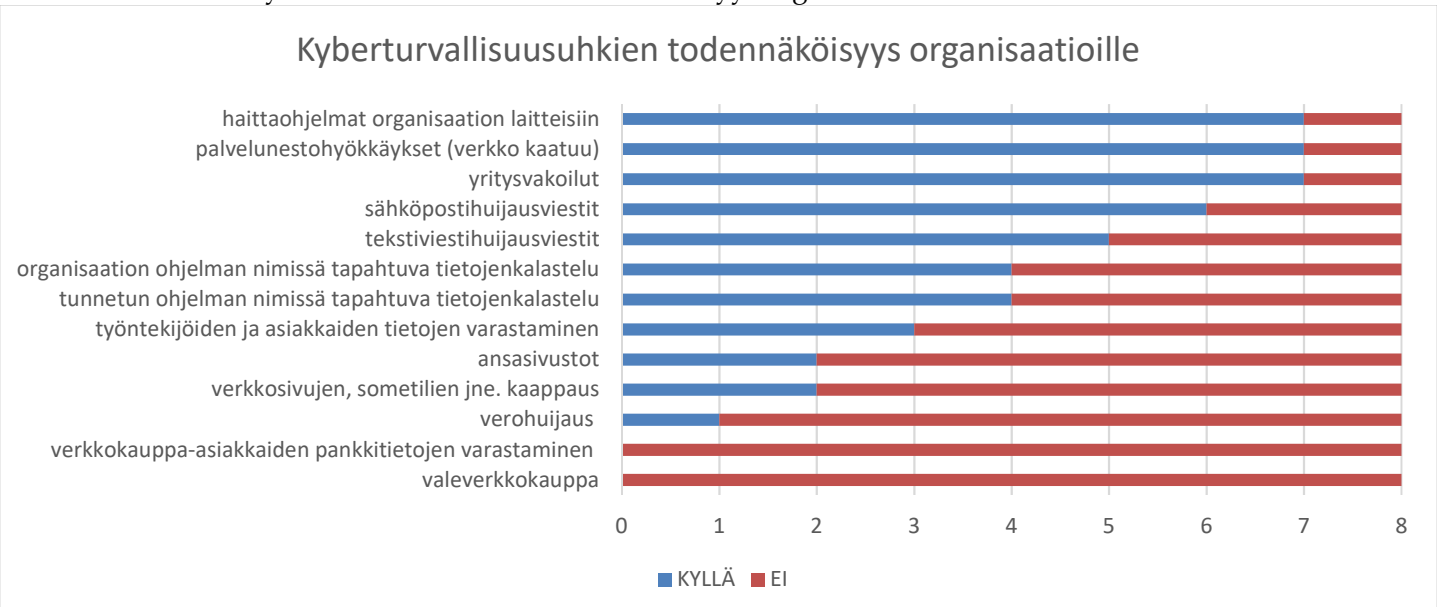
Viestinnän avoimuuden lisäksi viestinnän nopeus vaikutti erään vastaajan mielestä siihen, että yhteistyö koetaan turvalliseksi ja toisen mielestä taas se, että asiakkaille tehdään kyselyjä ja asiakaskokemusmittauksia. Muuan haastateltava piti myös hänen organisaatiossa toimitusjohtajan partneriviestinnän luovan turvallisuutta.

Kiinnostavaa on, että vain yksi haastateltava mainitsi luottamuksellisuuden tuovan turvallisuuden tunnetta. Mielenkiintoista on lisäksi se, että erään haastateltavan mielestä hänen organisaatiossa turvallisuutta ei tällä hetkellä ole tarvetta tuoda esille digitaalisessa ympäristössä ollenkaan, koska organisaation tuotetta myydään kasvokkain.

4.3 Kyberturvallisuusuhkat

Luotettavuuden jälkeen kysyttiin kyberturvallisuusuhkiin ja viestintään liittyviä kysymyksiä. Ensin haastateltaville lueteltiin 13 erilaista kyberturvallisuusuhkaa, ja jos haastateltavan mielestä joku uhka oli hänen organisaatiolle todennäköinen, tuli hänen vastata kyllä ja, jos taas uhka ei ollut todennäköinen, tuli vastata ei. Kootut tulokset ovat nähtävissä kaaviosta yksi. Kaaviossa sinisen palkin pituus kertoo, kuinka moni vastaajista piti kyseistä kyberturvallisuusuhkaa todennäköisenä eli mitä pidempi sininen viiva on, sitä useampi haastateltava piti uhkaa todennäköisenä. Vastaavasti mitä pidempi punainen viiva on, sitä useampi haastateltavista piti kyseistä uhkaa epätodennäköisenä.

KAAVIO 1. Kyberturvallisuusuhkien todennäköisyys organisaatiolle



Todennäköisimpinä kyberturvallisuusuhkina haastateltavat pitivät haittaohjelmia organisaation laitteisiin, seuraavaksi todennäköisempinä pidettiin palvelunestohyökkäyksiä ja kolmantena yritysvakoiluja. Erään haastateltavan mielestä yritysvakoilua tapahtuu tietyllä tasolla varmasti jatkuvasti. Suurin osa vastaajista piti myös tekstiviestihuijausviestejä todennäköisenä ja moni haastateltava koki, että joko oman tai tunnetun ohjelmistojen nimissä tehtävä tietojenkalastelu on todennäköistä. Enimmäkseen haastateltavat pitivät todennäköisenä organisaatiolleen kuutta tai seitsemää kyberturvallisuusuhkaa. Eräs haastateltava piti todennäköisenä 11 kyberturvallisuusuhkan toteutumista ja hän totesi:

> *"Kaikissa noissa (uhkissa) on se inhimillinen mahdollisuus, kun on se ihminen…että vaikka kuinka miettii asioita…ja meilläkin on sisäisesti ohjeistettu ja käyty läpi, mut ku aina on siinä se ihminen ja ihmiset ovat erehtyväisiä, niin kaikki on aina mahdollista. Et on tosi naivii sanoa, ettei meillä voi tapahtuu mitään."*

Tämän vastakohta oli eräs toinen haastateltava, joka piti todennäköisenä vain kahden uhkan toteutumista; palvelunestohyökkäyksien ja haittaohjelmien tarttumista organisaation laitteisiin, mutta oli kuitenkin sitä mieltä, että kaikki uhkat on silti otettava huomioon.

> *"…tokihan noita kaikkia uhkia mietitään, mä en niitä nää vaan todennäköisenä, mutta ei se tarkota, etteikö niihin pitäisi varautua…"*

Kukaan haastateltavista ei pitänyt todennäköisenä valeverkkokauppaa tai verkkokauppa-asiakkaiden luotto- ja pankkikorttitietojen varastamista. Tämä johtui siitä, ettei kellään organisaatiolla ollut verkkokauppaa. Lisäksi kovin todennäköisinä uhkina ei pidetty ansasivustoja tai organisaation verkkosivujen tai sosiaalisen median tilien kaappausta. Eräs haastateltava oli jopa sitä mieltä, ettei organisaatio voi tehdä kaappauksille mitään.

Annettujen vastausvaihtoehtojen jälkeen haastateltavalla oli mahdollisuus kertoa muita mahdollisia kyberturvallisuusuhkia. Usea haastateltava piti uhkana ihmisen omaa toiminta – joko asiakkaiden tahatonta tai tahallista toimintaa esim. tietoturvallisuuden laiminlyöntiä tai ylipäätään ihmisen inhimillisyyttä ja erehtyväisyyttä virheisiin. Erään haastateltavan vastaus poikkesi muista, sillä hän piti kyberturvallisuusuhkana sitä, ettei ole akreditoituja sertifikaatteja tietoturvaan liittyen ja siitä voisi muodostua kaupan este.

4.3.1 Pahin mahdollinen seuraus

Kyberturvallisuusuhkien todennäköisyyden selvittämisen jälkeen haastateltavalta kysyttiin, mikä olisi haastateltavan mielestä pahin mahdollinen seuraus organisaatiolle uhkan toteutuessa (kysymys 17). Vastauksissa tuli eniten esille pelko tietojen varastamisesta tai taloudellisista menetyksistä ja kolmantena pelko maineen menetyksestä.

Osa vastaajista piti asiakkaiden tietojen varastamista pahimpana, mutta osa sekä omien että asiakkaiden tietojen varastamista. Taloudellisista menetyksistä esimerkkinä mainittiin mm. GDPR -sanktio, joka on 4% globaalista liikevaihdosta.

Maineen menetystä pahimpana seurauksena pitäneistä eräs haastateltava sanoi, että mainetta on vaikea rakentaa uudestaan takaisin. Toisen mielestä sekä maineen menetys, että taloudellinen vastuu ovat yhtä pahoja seurauksia.

"Pahin mahdollinen olis taloudellisesti esim. gdpr-sanktio tulis…siinä on sitte se, että jos jotain tapahtuis, niin menee täysin uskottavuus ja maine…Molemmat on ikään kuin samalla tasolla..."

Vain yksi haastateltava mainitsi luotettavuuden menetyksen asiakkaiden silmissä pahimmaksi seuraukseksi.

Joukosta löytyi myös haastateltava, joka ei ajatellut pahimpana seurauksena taloudellista tappiota tai maineen menetystä, mutta jotka molemmat saattoivat olla vastauksen taustalla, sillä hän vastasi pahimmaksi seuraukseksi palvelun käytön estymisen. Lisäksi pahimmaksi seuraukseksi mainittiin lainsäädännöllinen vastuu, vaikeudet asiakkaalle ja omalle organisaatiolle sekä kilpailijan yritysvakoileman palvelun tulemisen markkinoille omaa organisaatiota aiemmin.

4.3.2 Kyberturvallisuusuhkat viestinnässä tällä hetkellä

Seuraavalla kysymyksellä, kysymyksellä 18, selvitettiin, miten haastateltavien mielestä todennäköisenä pidetyt kyberturvallisuusuhkat on huomioitu organisaation viestinnässä digitaalisessa ympäristössä.

Yleisesti voidaan sanoa, että vastaukset jakautuivat lähes kahtia, osan haastateltavien mielestä kyberturvallisuusuhkat eivät liity viestintään vaan kyse on teknologisesta asiasta.

"Kun ollaan teknologiayritys niin varaudutaan teknologian keinoin, eikä se sinällään liity viestintään…"

"…ei varsinaisesti viestinnässä ole sitä sillä tavalla huomioitu, eikä ole tarpeenkaan, vaan enemmän palveluitten rakentamisessa…"

"Me teemme enemmän kuin mitä meidän asiakkaat tietävät."

Oltiin myös sitä mieltä, että tällaiset asiat tulevat esille sopimuspapereissa, eikä niistä tarvitse erikseen viestiä. Erään haastateltavan mielestä heidän organisaatiossa ei ole edes löydetty keinoa viestiä kyberturvallisuusuhkista.

Osassa organisaatioita viestintää kyberturvallisuusuhkista kuitenkin oli. Joidenkin haastateltavien mielestä viestinnän tuli olla avointa ja aktiivista ja eräässä organisaatiossa kyberturvallisuusuhkat oli huomioitu myös viestintämallissa.

"Kyllä me suhteellisen aktiivisesti pyritään kertomaan, miten ollaan varauduttu…tuodaan esille meidän viestintämallilla, toisinaan kirjoitetaan niistä artikkeleita…"

"Asiakkaita opastetaan tietoturvassa…ku usein ne ongelmat on lähtöisin siitä, että asiakkaan päässä ei välttämättä huolehdita siitä tietoturvasta tarpeeksi… miten yritykset voivat parantaa omaa tietoturvaansa… ja sitten me itse tuodaan esille, miten me kehitetään tietoturvaa…ja henkilöstöä myös ohjeistetaan.."

Muutaman haastateltavan mielestä kyberturvallisuusuhkia ei huomioida oman organisaation viestinnässä tarpeeksi ja ne on huomioitu vain sisäisessä viestinnässä. Sisäisessä viestinnässä on kyberturvallisuudesta kouluttamista ja tietoturvasta muistutetaan yhtei-

sissä tilaisuuksissa. Vaikka muutamassa organisaatiossa kyberturvallisuusuhkat oli huomioitu sisäisen viestinnän lisäksi ulkoisessa viestinnässä, jotkut haastateltavat olivat sitä mieltä, että viestintä voisi olla silti nykyistä aktiivisempaa.

Eräs haastateltava oli huolissaan, ettei heillä ole riski- ja kriisiviestintäsuunnitelmaa, eikä ole nimetty henkilöitä, jotka ovat vastuussa viestinnästä, jos uhka toteutuu. Ainostaan yksi haastateltava toi esille, että organisaatiossa oli olemassa suunnitelmat.

> *" …meillä on tarkat suunnitelmat, niitten uhkien välttämiseen ja erilaiset suunnitelmat sit uhkiin reagoimiseen, jos jotain tapahtuu."*

Joissakin haastateltavien organisaatiossa uhkia oli pyritty torjumaan mm. tekemällä ennalta ehkäisevää työtä tietoturvaa kehittämällä tai lisäksi palkkaamalla hakkereita etsimään tietoturva-aukkoja. Niissä organisaatiossa, joissa uhkiin varautuminen tuli haastattelussa esille, siitä kerrottiin digitaalisissa sidosryhmäverkostoissa.

4.3.3 Miten kyberturvallisuusuhkat tulisi huomioida viestinnässä

Haastattelun viimeisessä kyberturvallisuusuhkiin liittyvässä kysymyksessä (kysymys 19) selvitettiin, miten haastateltavan mielestä kyberturvallisuusuhkat tulisi huomioida oman organisaation viestinnässä digitaalisessa ympäristössä.

Vastauksissa korostui eniten organisaatioiden sisäisen varautumisen tärkeys. Asiaa kuvailtiin kotipesän kuntoon laittamisella, tietoisuuden lisäämisellä, säännöllisenä muistutteluna ja parhaiden käytäntöjen kertaamisena organisaation sisällä. Eräs haastateltava toi esille, että heillä pitäisi laatia kriisiviestintäsuunnitelma ja nimetä vastuuhenkilöt viestintään. Hänen mielestä olisi myös tärkeää, että organisaatiolla on strateginen kumppani eli viestintätoimisto sille varalle, kun kriisi iskee.

Sisäisen varautumisen lisäksi vastaajat pitivät tärkeänä ulkoisen viestinnän parantamista ja yhteistyön lisäämistä. Eräs haastateltava sanoi:

> *"Kyllä me mun mielestä saatais olla vieläkin avoimempia…sais kertoa vielä avoimemmin näistä toimenpiteistä, sen eteen mitä he (konserniyhtiöt) tekee …, voitas tehdä sellasta yhteistyötä vähä kans enemmän…että tuotas vahvemmin esiin, millainen koneisto meillä on vastaamaan näihin uhkiin, mitä me tehdään niiden ennaltaehkäisemiseksi…meillä on todella vahva koneisto, joka siellä päivittäin näitä asioita seuraa työkseen…"*

Moni muukin haastateltava oli sitä mieltä, että sidosryhmille pitäisi ylipäätään viestiä nykyistä enemmän, mutta erityisesti nimenomaan kyberturvallisuusuhkista. Akuuteista kyberturvallisuusuhkista tulisi erään haastateltavan mielestä myös kertoa enemmän mm. siten, että mitä asiakas voi tehdä niiden torjumiseksi tai vähentämiseksi. Lisäksi tulisi tuoda esille kyberturvallisuuden hyödyt ilman liiallista pelottelua.

Viestinnän ymmärrettävyyttä pidettiin myös osan vastaajien mielestä tekijänä, joka tulisi huomioida kyberturvallisuudesta viestittäessä.

> *" …johon me viestintä kohdistetaan, ei tätä kokonaisuutta kovin hyvin ymmärrä, niin tässä mun mielestä viestinnässä on tärkeää, ett me pystytään muokkaamaan se viesti ymmärrettävään muotoon."*

Jos osa piti kyberturvallisuusuhkien esilletuomista tärkeänä, niin muutaman haastateltavan mielestä se ei ollut tarpeen. Eräs oli sitä mieltä, että viestiminen loisi enemmän uhkia ja esilletuominen voisi hyödyttää myös kilpailijoita.

> *"…se ei millään tasolla minun mielestä edistä sitä turvallisuutta tai enemmänkin se luo uhkaa…kilpailijat vois saada sellasta tietoa, mitä ne tarvii…"*

Tämä vastaaja oli myös sitä mieltä, että heidän organisaatiolle todennäköistä on vain kahden luetellun kyberturvallisuusuhkan toteutuminen; palvelunestohyökkäykset ja haittaohjelmat organisaation laitteisiin. Toisaalta on mielenkiintoista, ettei organisaatioissa nähty tarpeellisena kertoa, miten he turvaavat asiakkaille palvelun käytön, vaikka kyseiset kyberturvallisuusuhkat voivat vaikuttaa palvelun käyttöön.

4.4 Digitaaliset sidosryhmäverkostot

Digitaalisista sidosryhmäverkostoista oli alun perin tarkoitus kysyä kaksi kysymystä (kysymykset seitsemän ja kahdeksan); ketkä organisaatiosta viestivät ja ketkä vastaavat viestinnästä digitaalisissa sidosryhmäverkostoissa. Näiden kysymysten avulla oli tarkoitus selvittää, ketkä ovat näiden organisaatioiden toimijoita kyberympäristössä sidosryhmäverkostoissa ja ketkä vastaavat verkostojen viestinnästä. Lisäksi näiden kysymysten ja haastateltavien muiden vastausten perusteella oli tarkoitus luoda kuvaa, millaisia erilaisia toimijaverkostoja eli rihmastoja organisaatioilla on.

Haastattelun yhteydessä huomattiin, että osa mainitsi ulkomaille ja ulkomailla tapahtuvaa vuorovaikutusta, joten sitä päätettiin kysyä kaikilta haastateltavilta, jos he eivät tuoneet sitä vastauksissaan esille. Haastateltavilta saatettiin siten kysyä: onko organisaatiolla ulkomailla toimintaa ja kuinka laajasti? Haastateltavista osa toi esille myös kanavia, joissa verkostot toimivat, vaikka toimijaverkkoteorian mukaan verkostot ovat enemmänkin erilaisten aktanttien eli toimijoiden välisiä vuorovaikutusverkostoja, eikä niinkään kanavia. Jotta kaikilta haastateltavilta saatiin mahdollisimman samanlaiset tiedot, päädyttiin haastattelussa kysymään neljäs toimijaverkkoihin liittyvä kysymys: mitä digitaalisia sidosryhmäverkostoja organisaatiolla on.

4.4.1 Toimijat

Organisaatioiden toimijoita kyberympäristössä mainittiin osittain suoraan, mutta osa poimittiin haastateltavien puheista. Haastateltavissa SaaS-organisaatioissa digitaalisten sidosryhmäverkostojen toimijoita olivat:

- koko henkilöstö
- suurin osa henkilöstöstä
- markkinoinnin, myynnin ja viestinnän henkilöt
- organisaatio
- konserni

- tietoturva ja -suojan ammattilaiset
- asiantuntijat
- johto/toimitusjohtaja
- myynti- ja markkinointitiimit
- rekry- ja asiakassupporttiimit
- tuotekehitystiimin vetäjät
- ulkomailla olevat toimistot

Useiden haastateltavien mielestä organisaatioissa kaikki eli koko henkilöstö viestii ulospäin. Osa haastateltavista saattoi ensin vastata suppeammin, mutta muutama haastateltavaa palasi kysymykseen myöhemmin ja muutti vastaustaan siten, että kaikki loppupeleissä viestivät organisaatiosta ulospäin. Eräs vastaajista sanoi:

"Meiltä viestii valtaosa organisaatiosta. Me kannustetaan tosi aktiivisesti esim. sosiaaliseen mediaan."

Jotkut haastateltavista eritteliväät myös organisaation virallisen ja epävirallisen viestinnän. Jos nämä eriteltiin, virallisesti viestivät organisaation johto, markkinoinnin, myynnin ja viestinnän henkilöt sekä tietoturva ja -suojan ammattilaiset. Muu henkilökunta teki ns. epävirallista viestintää. Asiantuntijat olivat muutamien vastausten perusteella osana sekä epävirallista, että viralliseмpaa viestintää.

"Suurin osa jollain tapaa osallistuu… sitten on tietysti ammattilaisia, joiden työhön se kuuluu, että viestii aktiivisesti…jotka liittyy työhön ja työn tekemiseen…jokainen omalla tavallaan…"

"Kyllä kaikki tavalla tai toisella jollain tasolla viestii, mutta virallisemmin viestintä, markkinointi ja johto…on tietysti henkilöstö sinä myös mukana omalla tavallaan…mut jos puhutaan ihan virallisena yrityksen kanavana, niin sitten ne on nämä kolme."

Lisäksi joissakin organisaatioissa viestivät rekry- ja asiakassupporttiimit sekä tuotekehitystiimin vetäjät. Muutama haastateltava mainitsi puheessaan organisaation tai konsernin ja konsernin alaiset yhtiöt sekä toimistot / yksiköt ulkomailla. Organisaation koolla ei tuntunut olevan merkitystä, kuinka monen tai keiden kanssa haastateltavat kokivat viestivänsä.

4.4.2 Sidosryhmäverkostot

Tässä tutkimuksessa toimijaverkostot eli rihmastot käsitettiin ensisijaisesti organisaation ja sen ulkopuolella olevien toimijoiden välisinä digitaalisina sidosryhmäverkostoina. Silti tässä mainitaan myös haastatteluissa esiin tulleet organisaation sisäiset sidosryhmäverkostot.

Haastateltavien organisaatioilla oli ulkopuolisia sidosryhmäverkostoja useiden eri toimijoiden kanssa. Sidosryhmäverkostoja oli mm. asiakkaiden, alihankkijoiden, kumppaniyritysten, ulkopuolisten asiantuntijoiden, juristien, jälleenmyyjien ja muiden verkostolaisten kanssa. Verkostoja oli myös potentiaalisten työntekijöiden ja kilpailijoiden kanssa. Lisäksi oli maantieteellisiä verkostoja, esim. Suomessa, Suomesta Pohjoismaihin, Eurooppaan

ja yksittäisiin Euroopan maihin, Yhdysvaltoihin ja muihin lukuisiin maihin. Jos organisaatiolla oli toimisto tai myyjiä ulkomailla, voitiin siitä päätellä, että nämä organisaatiot muodostivat erilaisia toimijaverkostoja myös kyseisten maiden sisällä.

Lisäksi haastateltavien puheista oli poimittavissa verkostoja organisaatioiden sisällä. Siellä verkostoja oli yksittäisten ihmisten välillä, yrityksen perustajien kesken, tiimien sisällä ja tiimien kesken, johdon ja henkilöstön, asiantuntijoiden ja muun henkilökunnan välillä sekä konsernin sisällä olevien yhtiöiden välillä.

Kun haastateltavilta kysyttiin erikseen, mitä digitaalisia sidosryhmäverkostoja organisaatiolla on, nähtiin ne ensisijaisesti kanavina. Suurin osa haastateltavista puhui sosiaalisen mediasta: Twitteristä, Facebookista, LinkedInistä, Instagramista, blogeista ja eräs haastateltava mainitsi näiden lisäksi Snapchatin ja toinen haastateltava keskustelupalstat. Esille tuotiin myös organisaation verkkosivut, ja lisäksi useampi haastateltavaa mainitsi ainoastaan asiakkaille suunnatut omat kanavat.

"…community site on sitten meidän olemassa oleville asiakkaille."

"…enemmän materiaalia ja ne liittyy tarkemmin meidän palveluihin ja tuodaan esille työkaluja, …joita on meidän asiakkaiden käytössä, että on tukiportaali asiakkaiden käytössä…"

Digitaalisina sidosryhmäverkostoina nähtiin myös suorat ja nauhoitetut tapahtumat ja videoinnit. Haastateltavat mainitsivat mm. etäseminaarit, webinaarit, live streemaukset ja videot. Videoiden yhteydessä mainittiin Youtube ja Vimeo.

Sidosryhmäverkostojen yhteydessä osa vastaajista myös eritteli verkostoja virallisempiin ja epävirallisempiin. Esimerkiksi työntekijöillä ja asiantuntijoilla oli omia sosiaalisen median verkostoja, joissa toimittiin omilla nimillä, mutta tämän lisäksi asiantuntijat muodostivat virallisempia verkostoja organisaatioiden omissa kanavissa.

4.4.3 Digitaalisten sidosryhmäverkostojen edustajat organisaatiotasolla

Digitaalisten sidosryhmäverkostojen edustajia tiedusteltiin haastateltavilta kysymyksellä kahdeksan. Kysymys oli, ketkä vastaavat oman organisaation viestinnästä digitaalisissa sidosryhmäverkostoissa.

Viestinnänvastuuta oli monenlaista. Usein vastuu oli yrityksen johdolla, sillä monen vastaajan mielestä viestinnästä digitaalisissa sidosryhmäverkostoissa vastasi toimitusjohtaja. Eräässä organisaatiossa vastuu viestinnästä oli jaettu toimitusjohtajan ja hallituksen puheenjohtajan välillä eri osa-alueisiin. Haastatelluista henkilöistä strateginen johtaja ja viestintäjohtaja kokivat vastaavansa viestinnästä omissa organisaatioissaan, kuitenkin niin, että viestintäjohtaja vastasi konsernitason viestinnästä ja konserniyhtiöt omasta viestinnästään. Yhdessä organisaatiossa viestintävastuu oli hajautettu:

"…jokainen vastaa omasta osa-alueestaan, palvelutiimi palveluihin liittyvistä asioista lähinnä nykyasiakkaille, myynti- ja markkinointitiimi enemmän kaupallisesta viestinnästä ja minä (toimitusjohtaja) vastaan sijoittajaviestinnästä."

Eräässä organisaatiossa toimitusjohtaja sanoi ensin, että viestinnästä vastasi markkinointijohtaja, mutta lisäsi, että loppupeleissä hän vastaa viestinnästä. Muista vastaajista poiketen erään haastateltavan mielestä viestintävastuu digitaalisissa sidosryhmäverkostoissa oli organisaation myyntitiimin lisäksi alihankkijoilla.

5 JOHTOPÄÄTÖKSET

Tässä tutkimuksessa selvitettiin, miten SaaS-organisaatioissa nähdään kyberturvallisuusuhkien liittyvän luotettavuuteen ja maineeseen ja miten organisaatio voi pyrkiä vaikuttamaan organisaatioviestinnällä luotettavuuteensa kyberympäristössä. Tässä kappaleessa käsitellään, kuinka tutkimus vastasi sille asetettuihin tavoitteisiin, eli saatiinko tutkimuksella vastaukset tutkimuskysymyksiin. Lisäksi arvioidaan tutkimuksen yleistä onnistumista. Lopuksi vielä pohditaan, mitä hyötyä tutkimuksesta ja sen tuloksista on tulevaisuudessa.

5.1 Miten kyberturvallisuusuhkat liittyvät SaaS-organisaatioiden luotettavuuteen ja maineeseen?

Vastauksia ensimmäiseen tutkimuskysymykseen: *miten kyberturvallisuusuhkat liittyvät SaaS-organisaation luotettavuuteen ja maineeseen*, voidaan pitää hälyttävinä, sillä vain osa haastateltavista yhdisti kyberturvallisuusuhkat luotettavuuteen ja maineeseen.

Tutkimuksesta ensinnäkin ilmeni, että kyberturvallisuusuhkat voivat vaihdella organisaatioittain. Suurimassa osassa SaaS-organisaatiota pidettiin todennäköisenä useita kyberturvallisuusuhkia, mutta jotkut vastaajat pitivät todennäköisenä vain muutamaa uhkaa. Tulos on mielenkiintoinen, sillä Aljawarnehin (2017, 385) tutkimuksessa kyberiskuja pidettiin SaaS-organisaatioille lähes väistämättömänä asiana. Toisaalta on kuitenkin todettu, etteivät kaikki kyberturvallisuusuhkat ole kaikille samanlaisia (Kendrick 2010). Joko näissä vain muutamaa kyberturvallisuusuhkaa todennäköisenä pitävissä SaaS-organisaatioissa uhkat on huomioitu jo strategiassa ja niiden torjumiseksi on tehty enemmän töitä mitä haastattelussa kävi ilmi tai sitten organisaatioissa ei tunnisteta, että kyberturvallisuusuhkat ovat oikeasti todennäköisiä ja on tuudittauduttu jopa liialliseen turvallisuuden tunteeseen.

Moni haastateltava piti kuitenkin useaa kyberturvallisuusuhkaa organisaatiolle todennäköisenä. Jos uhka on todennäköinen, on se silloin merkki organisaation tai ihmisten haavoittuvuudesta (Hämäläinen 2018). Lisäksi maailman talousfoorumi (World Economic Forum) pitää kyberturvallisuusuhkia taloudellisten riskien lisäksi maineriskeinä (World Economic Forum 2015). Tutkimuksen SaaS-organisaatioissa taloudellisia menetyksiä pelättiin kuitenkin luotettavuuden ja maineen menetystä enemmän tai niitä ei mainittu mahdollisina riskeinä lainkaan.

Ehkä kyberturvallisuusuhkien yhteyttä maineeseen ja luotettavuuteen ei nähty siksi, että niitä pidettiin organisaation sisäisen viestinnän asiana ja ulkoisille sidosryhmille viestimistä pidettiin jopa tarpeettomana tai peräti vahingollisena tai niiden ei katsottu liittyvän viestintään lainkaan.

Hyvä asia on, että kaikki haastateltavat pitivät sisäistä varautumista tärkeänä ja kyberturvallisuusuhkat oli huomioitu teknologiassa, sillä ne ovat sisäisen viestinnän asia (Salman ym. 2016, 103, 105, 115, I-TU 2016, 17), mutta ainoastaan VTT:n raportti tukee ajatusta, ettei viestintä organisaation ulkopuolelle ole tärkeää (VTT 2017, 13). Myös Kendrick (2010, 126) pitää tärkeänä, että kyberturvallisuusstrategia jalkautetaan henkilöstölle, mutta ei ota kuitenkaan kantaa ulkoisten sidosryhmien viestintään.

Monessa SaaS-organisaatiossa kyberturvallisuuden eteen tehtiin enemmän töitä mitä kerrottiin. Kuitenkin Limnéll ym. (2014) ja ITU (2008, 2) pitävät kyberturvallisuusuhkia selkeästi kaikkien sidosryhmien asiana. ”*Kyberturvallisuus ei ole vain organisaation sisäinen asia vaan useita rajapintoja sisältävä jatkuva prosessi johon kuuluu lukuisia sidosryhmiä*” (Limnéll ym. 2014, 46). Lisäksi kyberturvallisuuteen liittyy luottamus eli, että jokainen hoitaa oman osansa turvallisuudesta (Limnéll ym. 2014, 40) ja viestintä on yksi keino lisätä luottamusta (MacMillan ym. 2005, 220-221; 228-229). Mutta, kuinka esimerkiksi asiakas voi luottaa organisaatioon, jos varautumisista ja suojautumisista ei kerrota tai heidän kyberturvallisuusosaamista ei lisätä tai edes selvitetä? Osassa SaaS-organisaatioita kuitenkin ymmärrettiin ulkoisen viestinnän ja sen avoimuuden merkitys ja osan mielestä kyberturvallisuusuhkista tulisi kertoa nykyistä avoimemmin. Tähän tulisi pyrkiä, sillä avoimuus on ”*paras maineenvarjelukeino*” (Limnéll ym. 2014, 83).

Mielenkiintoista on, että monessa SaaS-organisaatiossa viestintä kyberturvallisuusuhkista oli ulkoisille sidosryhmille vähäistä tai sitä ei ollut lainkaan, vaikka osa näin vastanneista oli sitä mieltä, että asiakkaiden tahaton tai tahallinen toiminta voi vaikuttaa kyberturvallisuusuhkien todennäköisyyteen. Kyberturvallisuusuhkiin liittyy ihmisten tahattomuus ja tahallisuus, ja uhka voi tulla sekä organisaation sisältä, että ulkoa (Limnéll ym. (2014, 23,37,106-107), joten ei riitä, että varautumista ja opastusta tehdään vain organisaatioiden sisällä. Kuten Limnéll ym. (2014, 107, 44) ovat sanoneet, tietoisuuden lisääminen on yksi parhaista kyberturvallisuusuhkiin varautumiskeinoista, ja ettei kyberturvallisuutta ole mahdollista luoda yksin.

Avoimemman viestinnän lisäksi tarvitaankin yhteistyötä. Haastateltavissa SaaS-organisaatioissa oli yhteistyötä eri sidosryhmien kanssa, mutta yhteistyö kyberturvallisuudesta tuli esille vain yhdessä organisaatiossa. Onneksi osa haastateltavista SaaS-organisaatioista pyrki vahvistamaan sidosryhmien osaamista kyberturvallisuusuhkista, sillä kaikkien verkostoissa olevien tulisi huolehtia verkoston turvallisuudesta (Salman ym. 2016, 108). Myös ANT:n mukaan toimijoiden yhteistyöllä voidaan estää odottamattomien tekijöiden pääsyä verkostoon (esimerkiksi viruksia tai trolleja), jotka voivat uhata verkoston vuorovaikutusta tai koko olemassaoloa (Kullman ja Pyyhtinen 2015, 118, 124). Siksi kaikkien verkostoissa olevien tulisi huolehtia verkoston turvallisuudesta (Salman ym. 2016, 108). Lisäksi on todettu, että suunnittelijoiden ja asiakkaiden välinen yhteistyö parantaa kyberturvallisuutta Aljawameh (2017, 385) ja yhteistyö on osa maineenhallintaa (Limnéll ym. 2014, 83).

Kyberturvallisuutta koskevassa viestinnässä tulee kiinnittää huomio ymmärrettävyyteen. Useat haastateltavat pitivät viestinnän ymmärrettävyyttä tärkeänä, vaikka se ei tullut suoraan esille kyberturvallisuuden osalta. Nursen ym. (2002, 61, 65-66) mukaan kybertur-

vallisuusuhkia käsittelevien kirjoitettujen viestien tulisi olla yksinkertaisia, hyvin suunniteltuja ja testattuja. Nursen ym. (2011) mainitsemalla viestien testaamisella ehkä vältyttäisiin siltä, ettei viestiminen menisi heti pelotteluksi, kuten eräs haastateltava totesi syyksi viestimättömyyteen kyberturvallisuusuhkista. Ymmärrettävyyden lisäksi kannattaa panostaa lisäksi viestinnän sisältöön, sillä sen sävy vaikuttaa maineeseen (Laaksonen 2004, 33).

Yhteenvetona voidaan todeta, että useissa tutkimuksen SaaS-organisaatioissa ei ymmärretä, että kyberturvallisuusuhkat voivat aiheuttaa taloudellisten riskien lisäksi maineja luotettavuusriskejä. Sisäinen viestintä ja teknologinen varautuminen olivat tulosten perusteella kunnossa, mutta tullakseen vahvemmiksi kyberturvallisuusuhkia vastaan, tulisi tutkimuksen SaaS-organisaatioissa kiinnittää enemmän huomioita sisäisen viestinnän lisäksi ulkoiseen proaktiiviseen organisaatioviestintään, koulutukseen ja yhteistyöhön sidosryhmien kanssa. Myös kyberturvallisuuden ja viestinnän tulisi olla osa organisaation strategiaa.

5.2 Miten viestinnällä voidaan vaikuttaa organisaation luotettavuuteen kyberympäristössä?

Toinen tutkimuskysymys oli: *Miten kyberympäristössä voidaan viestinnällä vaikuttaa organisaation luotettavuuteen.* Kysymykseen haettiin vastauksia kirjallisuudessa luotettavuutta kuvailevien määreiden avulla. Organisaatioilta kysyttiin, miten luotettavuus, rehellisyys, lakien ja sääntöjen noudattaminen, lisäarvon tuottaminen, asiantuntijuus ja osaamisen sekä turvallisuus tulevat esille organisaation viestinnässä kyberympäristössä.

Tutkimustulokset osoittavat, että useat SaaS-organisaatiot rakensivat luotettavuutta kyberympäristössä ensisijaisesti asiantuntijuudella, joka ilmenee asiantuntijasisältöinä. Sisältöä luotiin sekä omien että ulkopuolisten asiantuntijoiden kanssa mm. kertomalla omasta osaamisesta, palvelun ominaisuuksista ja alaan tai palveluun liittyvistä uudistuksista. Useimmiten sisällön tarkoituksena oli auttaa asiakkaita tai lisätä heidän yleistä tietämystä. Saas-organisaatioiden menetelmiä voidaan pitää viisaina, sillä Mae Kimin ja Brownin (2015, 10-12) mukaan asiantuntijuus eli oman asian osaaminen ja sen esilletuominen lisäävät uskottavuutta, joka on osa luotettavuutta (Pornpitakpan 2004, 269; Ohanian 1990, 39, 46, 50).

Useat tutkimuksessa mukana olleet SaaS-organisaatiot pyrkivät myös lisäämään luotettavuutta avoimuuden ja henkilöstön tunnistettavuuden avulla. Dasgupta ja Ferebee (2013, 5-6) ovat sitä mieltä, että avoimuus on erittäin tärkeää luottamuksen syntymiseen ja avoimuutta tulisi lisätä organisaatioissa entisestään. Verkkosivuilla organisaatioiden keino sitouttaa sidosryhmiä ovat avoimuus ja pääsy. Avoimuus tarkoittaa, missä määrin organisaatiosta kerrotaan ja pääsy taas sitä, kuinka erilaisilla viestintäkanavilla organisaatio on suoraan sidosryhmiensä tavoitettavissa (Shin ym. 2015, 186-187).

Luotettavuutta rakennettiin useimmissa tutkimuksen SaaS-organisaatoissa sisältömarkkinoinnilla. Howland ja Weis (1951) ovat todenneet, että viestin sisällöllä on merkitystä, miten luotettavana organisaatiota pidetään. Sisältömarkkinointi yritysmarkkinoinnissa (eli b2b = business to business -markkinoinnissa) tarkoittaa "*vakuuttavan ja ajankohtaisen sisällön luomista, jakamista ja levittämistä asiakkaille sitouttaen heitä ostamaan organisaatiolta sopivana ajankohtana.*" (Wangam, Malthouseb, Calderc, Uzunoglu 2017, 1-2; Holliman ja Rowley, 2014,

285). Wangam ym. (2017, 2) myös lisäävät, ettei sisältömarkkinointi kosketa suoraan yrityksen tuotetta. Useissa tutkimuksen SaaS-organisaatioissa pyrittiinkin lisäämään asiakkaiden yleistä tietämystä ilman, että se liittyi omaan tuotteeseen/palveluun.

Tutkimustulokset myös osoittivat, että monissa haastatelluissa SaaS-organisaatioissa luotettavuutta pyrittiin luomaan useilla eri keinoilla ja useissa eri kanavissa. Monipuolinen sisältö, jota viestitään eri tavoilla lisää luottamusta (Kuzhelev-Sagan ja Suchkoca 2016, 384, 389; Vernuccio 2014, 216). Silti ei saa unohtaa, että viestinnän tulisi olla yhteneväistä ja johdonmukaista organisaation muun toiminnan kanssa (Laaksonen 2014, 33). Ainakin muutamassa tutkimuksen SaaS-organisaatiossa viestintä pohjautui arvoihin, kulttuuriin ja tapaan toimia.

Viestinnän ymmärrettävyyttä ja sidosryhmälähtöisyyttä korostettiin useissa vastauksissa. Gefen ym. (2008) ovat tutkineet, että tekstit luovat kuvaa mm. organisaation hyväntahtoisuudesta ja rehellisyydestä, jotka liitetään kirjallisuudessa luotettavuuteen. Sisältöön panostaminen ja sen ymmärrettäväksi saaminen sidosryhmille on myös tärkeää siksi, että sisällön avulla pyritään luomaan tärkeitä merkityksiä sidosryhmille ja merkitysten luominen on tavoitteena luotettavuuden rakentamisessa (Lane ja Backhamn 2000, 75).

Lähes kaikissa tutkimuksen SaaS-organisaatioissa joko kaikki tai lähes kaikki osallistuivat viestintään kyberympäristössä. Organisaation henkilökunnan läsnäololla ja asenteilla on merkitystä organisaatioista syntyvään yrityskuvaan (Tran ym. 2015, 103). Lukuisten työntekijöiden viestimisestä voidaan puhua ns. työntekijälähettilyytenä eli kaikki tai moni henkilökuntaan kuuluva osallistuu organisaation viestintään. Se on myös kansainvälisen markkinointiviestinnän yritys Edelmanin (2017) mielestä erittäin hyvä tapa luoda sidosryhmien luottamusta. Työntekijälähettilyys tarkoittaa kuitenkin sitä, että organisaation johdon on luotettava henkilökuntaan. Luottamuksen rakentaminen työntekijöihin vaikuttaa tutkitusti organisaation maineeseen (Fombrun 1996, 28, 32, 72) ja yksi keino lisätä luottamusta henkilöstöön on työntekijälähettilyys. Organisaation sisäinen luottamus näkyy organisaatiosta ulos ja lisää luottamusta myös ulkoisissa sidosryhmissä.

Osa haastateltavista oli sitä mieltä, että luotettavuus syntyy vain tekojen tai asiakkaiden kautta. Tämä pitää sinällään paikkansa, että organisaation toimet vaikuttavat luotettavuuteen (Wiencierz ym. 2015, 103-104, 106, 113) ja, että digitaalisessa ympäristössä omakohtaiset kokemukset merkitsevät paljon (Dasgupta 2006, Sarojini 2015, Macmillan ym. 2005, 220-221; 228-229). Lisäksi sekä asiakastarinat että puheet luovat myös luottamusta (Lane ja Backham 2000, Edelman 2017), mutta kaikki edellä mainitut asiat eivät ole ainoita luotettavuuden rakentajia. Tutkimus osoitti, että niissä SaaS-organisaatioissa, joissa luotettavuuden nähtiin riippuvan pelkästään asiakkaista, ei viestinnällä koettu olevan suoraa vaikutusta organisaation luotettavuuteen kyberympäristössä. Organisaation viestinnällä on kuitenkin tutkimusten mukaan merkitystä sidosryhmien luottamukseen (MacMillan ym. 2005, 220-221, 228-229) ja internet on yksi tärkeimmistä markkinointiviestinnän kanavista SaaS-organisaatioille (Tyrväinen ja Selinin 2011, 6, 9).

Mielenkiintoinen havainto tutkimuksessa oli, että monet haastateltavat puhuivat tiedon jakamisesta kyberympäristössä, eivät vuorovaikutuksesta. Viestinnän ei pitäisi kuitenkaan olla vain yksisuuntaista organisaatiosta lähtevää, vaan sisältöä tulisi luoda yhdessä sidosryhmien kanssa, vuorovaikutuksessa (Vernuccio 2014, 214). Oikein toimittiin kuitenkin siinä, että osa organisaatioista auttoi asiakkaita ja he käyttivät monipuolisesti erilaisia keinoja sisällöntuottamisessa, sillä monipuoliset keinot ovat osa hyvää vuorovaikutusta (Vernuccio 2014, 216, 227). Hyvään vuorovaikutukseen kuuluu myös, millaista viestintä on

aktiivisuudeltaan ja muutoskyvyltään. Osa haastateltavista piti tärkeänä viestinnän säännöllisyyttä ja aktiivisuutta. Kyberympäristössä viestiminen vaatiikin vuorovaikutuksen lisäksi organisaatiolta nopeutta ja sopeutumiskykyä (ProCom 2012, Slabbert ja Barker 2014, 93) sekä joustavuutta (Spagnoletti ym. 2007, 1).

SaaS-toimialaan liittyvät monesta muusta toimialasta poiketen mm. erilaiset standardit ja säännöt. ISACAn mielestä sertifikaatit, ulkopuolisten auditoinnit sekä lakien ja säädösten noudattaminen ovat tärkeitä SaaS-toimialalla ja ne lisäävät organisaation luotettavuutta (ISACA 2009, 7). Tutkimustulosten perusteella osa tutkimuksen organisaatioista toi esille näitä viestinnässä, mutta eivät kaikki.

Yhteenvetona voidaan todeta, että useissa tutkimuksen SaaS-organisaatioissa organisaatioviestintää käytettiin monipuolisesti luotettavuuden rakentamisessa. Monet haastatellut organisaatiot toteuttivat viestintää sidosryhmälähtöisesti ja ymmärrettävästi monipuolisella asiantuntijasisällöllä eri keinoilla ja eri kanavissa. Organisaatiot, jotka eivät pitäneet viestintää tärkeänä luotettavuuden rakentajana, toivat kuitenkin kyberympäristössä esille muiden tavoin asiakkaita ja heidän tarinoita. Varsinainen vuorovaikutus sidosryhmien kanssa kuitenkin puuttui ja viestintä oli lähinnä yksisuuntaista tiedon jakamista. Useissa tutkimuksen SaaS-organisaatoissa luotettavuuden mielikuvaa voisi pyrkiä parantamaan entistä avoimemmalla viestinnällä, todellisella vuorovaikutuksella ja viestinnän strategisella johtamisella.

Tutkittavien SaaS-organisaation koolla ei tuntunut olevan tutkimuksen perusteella merkitystä, missä määrin viestinnän nähtiin luovan organisaation luotettavuutta. Lisäksi osa pienistä organisaatioista käytti yhtä monipuolisesti erilaisia menetelmiä ja kanavia luotettavuuden rakentamisessa mitä isoimmat organisaatiot.

5.3 SaaS-organisaatioiden digitaaliset sidosryhmäverkostot

ANT:n mukaan toimijaverkostojen eli sidosryhmäverkostojen koko ja erilaisuus voivat vaihdella (Ciustiniano ja Bolici 2012, 195). Tutkimuksen perusteella haastateltavissa SaaS-organisaatioissa oli sidosryhmäverkostoja useilla eri tasoilla ja eri laajuisena. Organisaation ulkopuolelle toimijaverkostoja oli yksilö-, tiimi, organisaatio- ja konsernitasoilla. Sen lisäksi oli maantieteellisesti muodostuneita verkostoja esim. Suomen sisällä ja Suomesta ulkomaille. Tutkimuksessa havaittiin myös verkostoja niiden virallisuuden mukaan ja samalle ne ilmaisivat eron toimijoiden välisestä voimakkuudesta. SaaS-organisaatioissa oli virallisia (ylin johto ja viestinnästä sekä markkinoinnista vastaavat -sidosryhmät) että epävirallisia (muu henkilöstö – sidosryhmät) verkostoja. Erikseen kysyttäessä haastateltavat näkivät digitaaliset sidosryhmäverkostot lähinnä sosiaalisen median erilaisina kanavina tai muotoina, jotka viestinnän kirjallisuudessa on nimetty digitaalisiksi vuorovaikutusareenoiksi ja jotka ANT:n mukaan ovat enemmän rakenteita eivätkä vuorovaikutussuhteita (Eriksson 2015, 40).

Merkille pantavaa tutkimuksessa oli, että vain yhdessä organisaatiosta tuotiin esille, että SaaS-palvelu itsessään luo vuorovaikutusta. Merkityksellistä tämä on siksi, että SaaS-organisaatioiden palveluita voidaan pitää ANT:n mukaisina ei-inhimillisinä toimijoina (Kullman ja Pyyhtinen 2015, 117), koska niiden kanssa asiakkaat ja SaaS-organisaatio, mutta myös mahdolliset kolmannet osapuolet, ovat yhteydessä. Toisaalta niitä voidaan pitää tekijöinä, jotka pitävät verkostoa yllä, jos ne ovat joillekin sidosryhmille tärkein asia esimerkiksi

asiakkuuteen. (Kullman ja Pyyhtinen 2015, 110, 118). SaaS-organisaatioissa ei joko nähdä, että palvelu luo ja ylläpitää sidosryhmäverkostoja tai sitten sitä pidetään liian itsestään selvänä mainittavaksi.

SaaS-organisaatioiden erikoisuutena ovat sertifikaatit, sopimukset ja lakien noudattaminen sekä ulkopuolisten auditoinnit ja, koska niillä on ISACAn (2009, 9) mukaan merkitystä organisaatioiden luotettavuuteen, voidaan niillä nähdä olevan merkitystä myös asiakkuuksien syntyyn, mutta myös merkitystä sidosryhmäverkostojen ylläpitämiseen. Suurimmassa osassa SaaS-organisaatioita näiden merkitys onkin ymmärretty ja niitä tuodaan esille viestinnässä.

ANT:n mukaan vuorovaikutus eli acting tai macroacting tapahtuu näkemättä toisiaan eri toimijoiden eli aktanttien kesken ja vuorovaikutus ja sen voimakkuus vaihtelee eri toimijoiden välillä (Latour 2007, 199-202). SaaS-organisaatioissa oli vuorovaikutusta sekä inhimillisten että ei-inhimillisten laitteiden välillä, mikä on kyberympäristön luonteen mukaista, samoin kuin se, että vuorovaikutus tapahtuu enimmäkseen näkemättä toisiaan ja sen voimakkuus voi vaihdella (Kullman ja Pyyhtinen 2015, 109).

Tutkimuksen SaaS-organisaatioissa vuorovaikutusta tapahtui sidosryhmäverkostoissa näkemättä toisia, mm. keskustelupalstoilla ja sähköpostien välityksellä. Joissakin haastateltavissa SaaS-organisaatioissa pyrittiin luomaan kuitenkin fyysisen maailman vuorovaikutusta kyberympäristöön mm. henkilöiden tunnistettavuudella; nimillä ja kuvilla, videoilla, webinaarien ja onlinekokousten avulla.

Tutkimuksen perusteella eniten vuorovaikutusta oli henkilökunnan ja asiakkaiden välillä. Asiakkaille oli joissakin organisaatioissa luotu jopa omia vuorovaikutuskanavia ja heille luotiin sinne tai muutoinkin laajempaa ja spesifimpää sisältöä. Tässä yhteydessä voidaan puhua myös luotettavuuden rakentamisesta, joka syntyy ANT:n mukaan vuorovaikutuksessa (Kullman ja Pyyhtinen 2015, 114). Luotettavuutta ulkoisiin sidosryhmiin pyrittiin SaaS-organisaatioissa ensisijaisesti rakentamaan asiantuntijuuden kautta ja panostus näkyi viestinnässä monipuolisina sisältöinä, tapoina ja kanavina. Myös kumppanuus asiakkaiden kanssa oli keino lisätä luotettavaa mielikuvaa organisaatiosta. Kumppanuusverkostoa voidaan pitää myös normaalia asiakassuhdetta vahvempana ja silloin molemminpuolinen luottamus on vahvempaa.

Kyberturvallisuusuhkat vaarantavat ANT:n sidosryhmäverkostojen vuorovaikutusta ja vakautta. Ne ovat toimijoita eli aktantteja, koska ne vaikuttavat verkostojen toimintaan (Balzacq ja Cavelty 2016, 176). ANT:n avulla voidaan tarkastella, miten verkostoissa ylläpidetään vakautta ja vahvistutaan uhkia vastaan (Crafword 2005, 1). SaaS-organisaatioissa vahvistuttiin niitä vastaan ensisijaisesti sisäisissä sidosryhmäverkostostoissa. Vain harvoissa haastateltavien vastauksissa tuli esille, että verkostoja tai vuorovaikutusta olisi organisaation ulkopuolisten sidosryhmäverkostojen kanssa. Balzacqin ja Caveltyn (2016, 176) mielestä kyberturvallisuusuhkat muokkaavat kyberympäristöä, mutta tässä tutkimuksessa ei noussut esille, että kyberturvallisuusuhkat olisivat muokanneet olemassa olevia SaaS-organisaatioiden sidosryhmäverkostoja.

ANT:n black box eli mustan laatikon tila on verkosto, jossa toimijat toimivat yhteen kestävästi ja luotettavasti (Kullman ja Pyyhtinen 2015, 118, 124). Latour (2007, 202) kuvaa mustan laatikon tilaa verkostossa sellaiseksi, että jos yksikin toimija muuttuu tai häviää, voi seuraukset verkostolle olla odottamattomat. Kyberturvallisuusuhkan, esimerkiksi haittaohjelman iskiessä SaaS-palveluun, olisi se yksi toimija lisää verkostossa ja se väistämättä horjuttaisi koko verkoston toimintaa. Suuntauksen mukaan mahdollisimman iskunkestävän

verkoston luomiseksi tarvitaankin samankaltaisia vuorovaikutustaitoja (Kullman ja Pyyhtinen 2015, 118, 124). Tutkimuksen perusteella osassa SaaS-organisaatioita ei ollut viestintää ja vuorovaikusta kyberturvallisuudesta ulkopuolisille sidosryhmille, joten vuorovaikutus ei voi siten olla samankaltaista, koska tietämys ja taidot voivat vaihdella. Samalla se tarkoittaa verkoston haurautta ja SaaS- organisaatioiden verkostossa ei voida katsoa tutkimuksen perusteella vallitsevan mustan laatikon tila.

5.3.1 Tutkimuksen arviointia

Tutkimuksen voidaan vastaavan sille asetettuihin tavoitteisiin, koska tutkimuskysymyksiin saatiin vastaukset, ja lisäksi voitiin kuvailla SaaS-organisaatioiden toimijaverkostoja.

Vastaavasti tutkimuksen rajauksen voi nähdä onnistuneen kohtuullisesti. Rajaus SaaS-organisaatioihin toimintaympäristön perusteella oli tutkimuksen kannalta hyvä ratkaisu, mutta henkilöstömäärän tai organisaation tuottaman palvelun osalta organisaatiot olisivat voineet olla enemmän heterogeenisia. Lisäksi viestinnän näkökulma olisi voinut tulla esille paremmin, jos olisi haastateltu pelkästään viestinnänammattilaisia.

Tutkimusta voidaan pitää onnistuneena myös siksi, koska se vastasi tutkimuksessa asetettuihin tavoitteisiin. Haastattelu oli tutkimuksessa toimiva tiedonkeruumenetelmä, mutta vähemmällä haastateltavien ja kysymysten määrällä olisi voitu kuitenkin haastatella syvällisemmin, jolloin olisi voitu pureutua paremmin kyberturvallisuuden ja viestinnän teemoihin. Myöskään ei voida olla varmoja, kärsikö tutkimuksen luotettavuus, koska haastateltavilla on tapana antaa vastauksia, jotka ovat soveliaita (Hirsjärvi, Remes Hurme, 2009, 206). Haastateltavat kuitenkin tiesivät, ettei henkilö tai organisaatio tule esille missään raportointivaiheessa, joten tämä saattoi vaikuttaa vastaajien rehellisyyteen positiivisesti. Toisaalta raportointivaiheessa on mahdollista, että tutkija vaikuttaa tutkittavilta saatuihin tietoihin (Kiviniemi 2015, 77-79), vaikka pyrkimyksenä tulisi aina olla, että ymmärretään tutkittavien käyttämiä sanavalintoja ja merkityksiä (Swanson ja Holton 2005, 234).

Tämä tutkimus on onnistunut myös siksi, että se on tuonut uutta tietoa useille tieteenaloille. Tutkimuksen voidaan tuoneen kyberturvallisuutta ja -uhkia käsittelevään tutkimukseen tietoa siitä, että kyberturvallisuus koskee kaikkia ja että viestintä, maine ja luotettavuus ovat osa kyberturvallisuutta. Viestinnän tutkimukselle tämä antaa vastaavasti tietoa siitä, miten kyberturvallisuusuhkat liittyvät organisaation maineeseen, luotettavuuteen sekä organisaation sisäiseen ja ulkoiseen viestintään. Tutkimus antaa myös lisävahvistusta siihen, että kyberturvallisuusuhkat tulisi huomioida viestintästrategiassa ja riski- ja kriisiviestintäsuunnitelmissa. Lisäksi tutkimus osoittaa, että sekä luotettavuuden että kyberturvallisuuden vahvistamiseen tarvitaan sidosryhmälähtöisyyttä ja avointa viestintää eri keinoin eri kanavissa. Lisäksi tutkimus antaa kootusti lisätietoja luotettavuuden ja maineen rakentamisesta kyberympäristössä. Yritysten johdolle tutkimus tarjoaa tietoa siitä, kuinka sekä kyberturvallisuusuhkat että viestintä tulisi olla osa strategiaa. SaaS-organisaatioita tämä puolestaan auttaa ymmärtämään viestinnän ja kyberturvallisuuden merkityksen luotettavuuden ja maineen rakentamisessa kyberympäristössä.

Tämä tutkimus osoitti, että kyberturvallisuutta, organisaatioiden luotettavuutta ja mainetta yhdistävää tutkimusta olisi tärkeää tutkia myös jatkossa mm. eri toimialoilla ja isommassa tutkimusjoukossa. Saman haastattelututkimuksen voisi toteuttaa suuremmalle joukolle SaaS-organisaatioita tai tutkimuksen pohjalta voisi tehdä määrällisen tutkimuksen

koko toimialalle. Mielenkiintoinen jatkotutkimusaihe voisi myös olla, millä tavalla kyberturvallisuusuhkien nähdään vaikuttavan maineeseen ja luotettavuuteen toimialoilla, joissa tuote tai palvelu ei ole kyberympäristössä. Lisäksi uusissa tutkimuksissa voisi toimitusjohtajien sijaan haastatella pelkästään viestinnänammattilaisia tai IT- ja kyberturvallisuusasiantuntijoita. Toisaalta taas riski- ja kriisiviestinnän puolella voisi tutkia, miten kyberturvallisuusuhkat on huomioitu organisaatioiden riski- ja kriisiviestintäsuunnitelmissa.

6 KÄYTÄNNÖN SUOSITUKSIA

Käytännön suositukset ovat yleisiä ehdotuksia kyberturvallisuuden ja viestinnän parantamiseksi tutkimukseen osallistuneille SaaS-organisaatiolle. Suosituksia ei voi pitää kaikenkattavina ohjeina, mutta ne antavat hyvät peruslähtökohdat viestinnän tekemiseen ja mielikuvien muodostumiseen kyberympäristössä. Vaikka maine ei ole täysin organisaation hallittavissa (Luoma-Aho ja Vos 2010, 322), voi organisaatio silti vaikuttaa osittain toimillaan siihen, millainen mielikuva siitä on ja miten maine rakentuu (Wiencierz ym. 2015, 103-104, 106, 113).

Kyberturvallisuus ja viestintä osaksi kaikkea toimintaa

Kyberturvallisuuteen että viestintään liittyvän luotettavuuden ja maineen rakentaminen tulisi lähteä organisaation kulttuurista, arvoista ja strategiasta (Wiencierz ym. 2015, 103-104, 106, 113; Mae Kim ja Brown (2015, 10-12); Tran ym. 2015, 102; Slabbert ja Barker 2014, 93). Kyberturvallisuuden ja viestinnän tulisikin olla osa strategiaa (Limnéll ym. 2014, 14, 24, 56-57, 74, 161; Falkheimer 2014, 127).

Arvoista lähtevä organisaatioviestintä tulisi lisäksi integroida kaikkeen yrityksen toimintaan. Silloin viestintä on yhtenäistä ja koko organisaation viestintätoimet tukevat organisaation liiketoimintatavoitteita. Integroitu viestintä voi myös parantaa esimerkiksi verkkoviestinnän kampanjoiden koordinointia ja reaaliaikaisten tapahtumien viestintää. (Gurau 2013, 533.)

Kyberturvallisuusuhkien osalta tulisi tehdä riskienhallintaa (IRM 2018) ja varautua uhkien toteutumiseen tekemällä yhteistyötä sidosryhmien kanssa (ITU-T 2008, 2). Lisäksi tulisi luoda riski -ja kriisiviestintäsuunnitelmat. Riskienhallinta ja siitä sidosryhmille kertominen voisivat olla myös tapa erottua kilpailijoista (IRM 2018).

Riskienhallinnan lisäksi tarvitaan riskiviestintää. Riskiviestintä on ennen kriisiä tapahtuvaa viestintää, jossa organisaatio käy kaikkien sidosryhmiensä kanssa jatkuvaa keskustelua ja tiedonvaihtoa mahdollisista negatiivisista organisaation toimintaa uhkaavista tekijöistä, riskeistä ja niiden torjumisesta ja tunnistamisesta (Lehtonen 2009, 31-32).

Kuten nähdään, tulisi kyberturvallisuus ja viestintä huomioida kaikessa ja olla osa jokapäiväistä organisaation toimintaa.

Tavoitteellista ja monipuolista viestintää resursseja unohtamatta

Strategian jälkeen tulee tehdä varsinaiset suunnitelmat siitä, kuinka strategia toteutetaan käytännössä. Se tarkoittaa toimenpiteiden konkreettista miettimistä ja aikataulutusta (Steyn, 2004, 175). On mietittävä, mikä on organisaation tavoite ja resurssit (henkilöt, osaaminen, aika, raha) (Zerfass ja Viertmann 2017, 22). Esimerkiksi sosiaalisen median kanavien ylläpito, monitorointi ja vuorovaikutus digitaalisessa ympäristössä vaativat osaamista, mutta myös aikaa (Slabbert ja Barker 2014, 93; Limnéll ym. 2015, 203). Lisäksi on luotava mittaristot tavoitteiden saavuttamisen seuraamiseen ja huomioitava sekä lyhyen että pitkän aikavälin tavoitteet. Mittareita suunnitellessa on tärkeää valita sellaisia mittareita, jotka mittaavat sitä mitä halutaan (Vos 2011, 224, 229, 236, 238.).

Sidosryhmien tuntemus määrittää viestinnän sisällön

Käytännön suunnitelmien onnistumiseksi tarvitaan tieto, kenelle ja kenen kanssa viestintää tehdään. Monitorointi on keino, jolla saadaan selville, missä halutut sidosryhmät ovat, keitä he ovat, mikä heitä kiinnostaa ja mistä he keskustelevat. Monitorointi on kyberympäristössä välttämätöntä ja jatkuvaa toimintaa (Strauβ ja Jonkman 2017, 34-35). Monitoroinnin lisäksi kannattaa hyödyntää myös perinteisempiä kyselyjä, asiakas -tai sidosryhmätyytyväisyyskyselyitä, jotka ovat helppoja ja nopeita toteuttaa digitaalisessa ympäristössä. Monitorointeja ja kyselyjä on hyvä tehdä tarpeeksi säännöllisesti, jotta pystytään paremmin vastaamaan ympäristön muutoksiin ja siten turvaamaan oma liiketoiminta (Slabbert ja Barker 2014, 92). Kun sidosryhmät tunnetaan paremmin, on helpompaa miettiä organisaatioviestinnän sisältöä, keinoja ja kanavia (Shin ym. 2015, 200).

Monipuolinen viestintä, sidosryhmälähtöisellä sisällöllä oikeilla keinoilla ja oikeissa kanavissa on tapa lisätä luottamusta (Kuzhelev-Sagan ja Suchkoca (2016, 384, 389; Vernuccio 2014, 216, Limnéll ym. 2015, 203). Sisältöön panostaminen ja sen ymmärrettävyys on merkittävää myös siksi, että sisällön avulla pyritään luomaan tärkeitä merkityksiä sidosryhmille ja lisäksi se on luotettavuuden rakentamisen tavoitteena (Lane ja Backhamn 2000, 75). Ymmärrettävyys on tärkeää myös kyberturvallisuusviestinnässä (Nurse ym. 2011, 61, 65-66).

Lisää vuoropuhelua ja yhteistyötä

Viestinnän kanavat, keinot ja sisältö ei kuitenkaan riitä. Lisäksi tarvitaan vuoropuhelua. Tutkimukseen osallistuneissa organisaatioissa vuorovaikutus oli lähinnä tiedon jakamista ja välittämistä, ei aitoa vuoropuhelua – tai ainakaan todellinen vuoropuhelu ei tullut esille.

Vuorovaikutus tarkoittaa vuoropuhelua, ja aito vuoropuhelu ei ole yksisuuntaista tiedonjakamista (ProCom 2012; Luoma-Aho ja Vos 2010, 322; Vernuccio 2014, 214; Coombs ja Holladay 2015, 691). Aito vuorovaikutus on tärkeää, koska sen avulla syntyy luottamusta. Eräs tapa lisätä vuorovaikutusta on esimerkiksi avointen kysymysten esittäminen sosiaalisessa mediassa ja omissa asiakaskanavissa. Sidosryhmiä voi myös kannustaa jakamaan sisältöä organisaation omilla kanavilla. Ainoastaan yhdessä tutkimukseen osallistuneista organisaatoista osallistuttiin yhteiskunnalliseen keskusteluun, vaikka myös se on erinomainen keino osallistua vuoropuheluun, luoda tunnettuutta ja myös osoittaa asiantuntijuutta (Vernuccio 2014, 214) ja asiantuntijuuden kautta luoda luottamusta (Pornpitakpan 2004, 269,

Ohanian 1990, 39, 46, 50). Kuten Vernuccio (2014, 221) on todennut, tulisi vuoropuheluun osallistua myös koko henkilökunta eri sidosryhmien kanssa. Aiemmin mainituilla monitoroinnilla ja mittareilla voidaan seurata ja selvittää, mitkä vuorovaikutustavat ovat lisänneet luottamusta parhaiten (Lane ja Backhamn (2000, 75) ja jotka vaikuttavat myös positiivisesti maineeseen.

Aiempien tutkimusten ja kirjallisuuden perusteella voidaan myös sanoa, että luotettavuuden rakentaminen, olipa kyse kyberturvallisuudesta tai ei, tarkoittaa myös kumppanuutta ja yhteistyötä (Limnéll ym. 2014, 83; Aljawarneh 2017, 385; Dasgupta ja Ferebee 2013, 58). Tutkimuksen SaaS-organisaatioissa tulisikin lisätä tai aloittaa tiiviimpi yhteistyö edes tärkeimpien ulkoisten sidosryhmien kanssa. Yhteistyössä kannattaa miettiä omia asiakkaita, yhteistyöyrityksiä ja alihankkijoita laajemmin mm. yhteistyötä alan sisällä, alueellisesti ja valtakunnallisesti (Dasgupta ja Ferebee 2013, 61, 63). Lisäksi organisaatioiden kannattaa kiinnittää huomioita, keiden kanssa yhteistyötä tehdään eli kumppaneiden tulisi sopia yrityksen arvoihin ja kulttuuriin ja siihen, miksi ollaan olemassa ja mihin halutaan päästä (Vernuccio 2014, 228).

Avoimuus on osa viestintää ja kyberturvallisuutta

Kun viestintä on osa strategiaa, lisää se organisaation avoimuutta sekä organisaation sisällä että sieltä ulospäin (Falkheimer 2014, 130-131). Avoimuus on keino, jolla voidaan kehittää varautumista kyberturvallisuusuhkia vastaan (Limnéll ym. 2015, 83), mutta myös lisätä luottamusta (Dasgupta ja Ferebee (2013, 5-6, ProCom 2012). Avoimuus kyberturvallisuusuhkista ulkoisille sidosryhmille oli heikkoa haastateltavissa SaaS-organisaatioissa, joten tullakseen vahvemmiksi uhkia vastaan, organisaatioiden tulisi sisäisen varautumisen lisäksi viestiä niistä myös ulkoisille sidosryhmille.

Tälle vuodelle eli vuodelle 2018 Suomen kyberturvallisuuskeskus on ennustanut, että avoimuus kyberturvallisuusuhkista lisääntyy ja että enää ei pelätä maineenmenetystä uhkien esilletuomisessa (Viestintävirasto julkaisu 001/2018, 28). Tämä on jossain määrin ollut nähtävissä, kuten tässäkin työssä esille nostetut Uberin, Metsä-Groupin ja Provincian esimerkit todistavat. Toivottavasti tämä tarkoittaa myös viestinnän merkityksen ymmärtämistä osana kyberturvallisuutta. Kuten eräs haastateltava totesi: *"Siellä on se teknologia… ja sitten on myös se ihminen."*

KIRJALLISUUS

Alasuutari, P. (2011). *Laadullinen tutkimus 2.0* (4. uud. p.). Tampere: Vastapaino.

Aljawarneh, S. A. (2017). Cloud security engineering: Early stages of SDLC. *Future Generation Computer Systems*, 74, 385–392.

Aula, P. ja Heinonen, J. (2002). *Maine: Menestystekijä.* Helsinki: WSOY.

Aula, P. ja Mantere, S. (2006). *Hyvä yritys: Strateginen maineenhallinta*. Helsinki: WSOYpro.

Aula, P. (2000). *Johtamisen kaaos vai kaaoksen johtaminen?* Porvoo ; Helsinki ; Juva: WSOY

Balzacq, T. ja Dunn Cavelty, M. (2016). *A theory of actor-network for cyber-security*. European Journal of International Security, 1, part 2, 176–198. British International Studies Association 2016

Belliger, A. (2016). *Organizing networks: An actor-network theory of organizations*. Bielefeld, GERMANY: Transcript Verlag.

Bersoff, D.M. (2017). *Every business needs to be trust-aware*. Saatavilla www-muodossa https://www.edelman.com/post/every-business-needs-trust-aware. (6.2.2018).

Brookson, C., Cadzow, S.,Eckmaier, R., Eschweiler, J.,Gerber, B.,Guarino, A., Rannenberg, K.,Shamah, J. ja Górniak, S. (2016). *Definition of Cybersecurity - Gaps and overlaps in standardisation*. European Union Agency For Network And Information Security.

Castelfranchi, C. ja Tan, Y-H. (2002). The Role of Trust and Deception in Virtual Societies. International Journal of Electronic Commerce, 6(3), 55–70.

Coombs, T, W. ja Holladay, S.J. (2015). Public relations' "Relationship Identity" in research: Enlightenment or illusion. *Public Relations Review, 41*(5), 689–695.

Cornelissen, J. P. (2017). *Corporate communication: A guide to theory and practice* (5th edition.). London: SAGE Publications Ltd.

Correia Loureiro, S., Kaufmann, H. R., Rabino, S. (2014). Intentions to use and recommend to others. *Online Information Review, 38*(2), 186–208.

Dasgupta, S. (2006). *Encyclopedia of virtual communities and technologies.* Hershey, PA: Idea Group Reference

Dasgupta, D. ja Ferebee, D.M. (2013). *Consequences of Diminishing Trust in Cyberspace*. International Journal of Cyber Warfare and Terrorism (IJCWT), 3(3), 19–31.

Edelman. (2017). Verkkojulkaisu. 10 trust barometer insights. Saatavilla www-muodossa https://www.edelman.com/10-trust-barometer-insights (6.2.2018)

Elling, M. ja Shcnell, W. (2016). *What do we know about cyber risk and cyber risk insurance?* The Journal of Risk Finance, 17(5), 474–491.

ENISA (2017). *Guidelines for TSPs based on standards. Techinal guidelines on trust services*. European Union Agency For Network And Information Security.

Eriksson, K. (2015). *Verkostot yhteiskuntatutkimuksessa*. [Helsinki]: Gaudeamus.

Falkheimer, J. (2014). The power of strategic communication in organizational development.*International Journal of Quality and Service Sciences, 6*(2/3), 124–133.

FiCom. Tietopaketti kyberympäristöstä. Saatavilla www-muodossa https://www.ficom.fi/sites/default/files/pictures/Kyberymp%C3%A4rist%C3%B6_kyberturvallisuus_ei-kyber-ihmisille.pdf (28.11.2017)

Foroudi, P. ja Montes, E. (2017). Corporate e-communication: Its Relationship with Corporate Logo in the Construction of Digital Interaction Platforms. *The Bottom Line*, 201–215.

Gefen, D., Benbsati, I. ja Pavlou, PA. (2008). *A research agenda for trust in online environments*. Journal Of Management Information Systems, 24(4), 275–286.

Giustiniano, L. ja Bolici, F. (2012). Organizational trust in a networked world. *Journal of Information, Communication and Ethics in Society*, 10(3), 187–202.

Grigorescu, A. ja Lupu, M-M. (2015). Integrated Communication as Strategic Communication. *Revista de Management Comparat International, 16*(4), 479–490.

Gotsi, M. ja Wilson, A. M. (2001). Corporate reputation: Seeking a definition. Corporate Communications: *An International Journal*, 6(1), 24–30.

Gurău, C. (2013). Developing an environmental corporate reputation on the internet. *Marketing Intelligence ja Planning*, 31(5), 522–537.

Hatch, M. ja Shultz, M. (2003). Bringing the corporation into corporate branding. *European Journal of Marketing, 37*(7/8), 1041–1064.

Hirsjärvi, S. ja Hurme, H.(2000). *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö*. Helsinki: Yliopistopaino.

Hirsjärvi, S., Remes, P. Sinivuori, E. (2009). *Tutki ja kirjoita* (15. uud. p.). Helsinki: Tammi.

Howland, C. I. ja Weiss, W. (1951). The Influence of Source Credibility on Communication Effectiveness. *The Public Opinion Quarterly* 15 (4), 635–650.

IDC (2017) Worldwide Public Cloud Services Revenue Growth Remains Strong Through the First Half of 2017, According to IDC. Business Wire. Saatavilla www-muodossa https://www.businesswire.com/news/home/20171106005140/en/Worldwide-Public-Cloud-Services-Revenue-Growth-Remains (27.2.2018)

IRM. (2018) Institute of Risk Management. Saatavilla www-muodossa https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk.aspx (12.1.2018)

ISACA (2009). *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives.* An ISACA Emerging Technology White Paper.

International Telecommunication Union. (2008). *Series x: Data networks, open system communications and security*. Telecommunication security. Overview of cybersecurity. Recommendation ITU-T X.1205.

Kendrick, R. (2010). *Cyber risks for business professionals: A management guide*. Ely: IT Governance Pub

Ki, E. ja Hon, L.C. (2007). Reliability and Validity of Organization-Public Relationship Measurement and Linkages among Relationship Indicators in a Membership Organization. *Journalism ja Mass Communication Quarterly*, 84(3), 419–438.

Kramer, R. M. ja Cook, K. S. (2004). *Trust and distrust in organizations: Dilemmas and approaches*. New York: Russell Sage Foundation.

Kramer, R. M. ja Tyler, T. R. (1996). *Trust in organizations: Frontiers of theory and research*. Thousand Oaks (CA): Sage.

Kullman, K. ja Pyyhtinen, O. (2015). Toimijaverkosto. Toim. Eriksson, K. (2015). *Verkostot yhteiskuntatutkimuksessa*. [Helsinki]: Gaudeamus.

Kuzheleva-Sagan, I. ja Suchkova, N. (2016). Designing trust in the Internet services. *AI ja SOCIETY*, 31(3), 381–392.

Laaksonen, S-M. (2014). Särkymätön tunnepääoma. Toim. Luoma-aho, V. ja Karvonen, E. (2014). *ProComma Academic 2014: Särkymätön viestintä*. Helsinki: ProCom - Viestinnän ammattilaiset ry.

Lane, C. ja Bachmann, R. (2000). *Trust within and between organizations: Conceptual issues and empirical applications* ([Rev. ed.].). New York: Oxford University Press.

Lassila, A. Helsingin sanomat. (9.1.2018). ”Metsä Group: Yrityksen järjestelmiin on ehkä murtauduttu ja arvokkaat tulostiedot ovat voineet vaarantua – ”Tämä tilanne on edelleen päällä”. Saatavilla www-muodossa https://www.hs.fi/talous/art-2000005517989.html (9.1.2018.)

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford ; New York: Oxford University Press.

Latvakoski, J. (ja Röning, J.) (2016). *Small world for dynamic wireless cyber-physical systems*. Technical Research Centre of Finland (VTT).

Lehto, M. ja Kähkönen, A. (2015). *Kyberturvallisuuden kansallinen osaaminen*. Jyväskylä: Jyväskylän yliopisto

Lehto, M. ja Neittaanmäki, P. (2014). *Kyberturvallisuuden ja big data-analyysin tutkimus ja opetus*. Jyväskylä: Jyväskylän yliopisto.

Lehtonen, J. 2009. Ettei pahin tapahtuisi – Riski- ja kriisiviestinnän perusteet. Helsinki: Ykkös-Offset.

Limnéll, J., Majewski, K. ja Salminen, M. (2014). *Kyberturvallisuus*. Jyväskylä: Docendo.

Littlejohn, S. W. ja Foss, K. A. (2009). *Encyclopedia of communication theory*. Thousand Oaks, Calif.: Sage.

Luppicini, R. (2014). Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research. *Global Media Journal*, 7(1), 35–49.

Lönnqvist, I. ja Moilanen, P. (2017). *Kyberin taskutieto – Keskeisin kybermaailmasta jokaiselle*. Jyväskylä: Jyväskylän Yliopisto ja Maanpuolustuskoulutusyhdistys.

Mae Kim, C. ja Brown, W. J. (2015). *Conceptualizing Credibility in Social Media Spaces of Public Relations*. Public Relations Journal, 9, No. 4.

McGinnies, E. ja Ward, C. (1980). Better Liked Than Right: Trustworthiness and Expertise as Factors in Credibility. *Personality and Social Psychology Bulletin*, 6(3), 467

Macmillan, K., Money, K., Downing, S., Hillenbrand, C. (2005). Reputation in Relationships: Measuring Experiences, Emotions and Behaviors. *Corporate Reputation Review*, 8(3), p. 214.

Maister, D. H., Green, C. H. ja Galford, R. M. (2012). *Luottamuksen arvoinen*. Helsinki: Talentum.

Manning, P. K. (1992). *Organizational communication*. New York: Aldine de Gruyter.

Mayer, R., Davis, J. ja Schoorman, F.D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, 20(3), 709.

Mezgár, István. (2006). Trust in Virtual Organizations. Toim. Dasgupta, S. (2006). *Encyclopedia of virtual communities and technologies.* Hershey, PA: Idea Group Reference

Miller, G. R., Baseheart, J. (1969). Source trustworthiness, opinionated statements, and response to persuasive communication. *Speech Monographs*, 36(1), 1–7.

Navarro, C., Morena, A., Al-Sumait, F. (2017). Social media expectations between public relations professionals and their stakeholders: Results of the ComGap study in Spain. *Public Relations Review*, 43(4), 700–708.

Newcomer, E. Bloomberg. (21.11.2017). Uber paid hackers to delete stolen data on 57 million people. Saatavilla www-muodossa

https://www.bloomberg.com/news/articles/2017-11–21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data (26.11.2017)

Nurse, J. R. C., Creese, S., Goldsmith, M. ja Lamberts, K. (2011) *Trustworthy and effective communication of cybersecurity risks*. A review. Socio-Technical Aspects in Security and Trust (STAST), 2011 1st Workshop, 60–68.

Ohanian, R. (1990). Construction and validation of a scale to measure celebrity endorsers' perceived expertise, trustworthiness, and attractiveness. *Journal of Advertising* 19 (3), 39-52

Ojala, A. (2013). Software-as-a-Service Revenue Models. *IEEE Computer Society*.

Olkkonen, L. ja Luoma-aho, V. (2015). Broadening the Concept of Expectations in Public Relations. *Journal of Public Relations Research, 27*(1), 81–99.

Oxford Reference Online. Saatavilla www-muodossa http://www.oxfordreference.com.ezproxy.jyu.fi (30.11.2017)

Pang, A., Shin, W., Lew, Z. ja Walther, J.B. (2018). Building relationships through dialogic communication: Organizations, stakeholders, and computer-mediated communication. *Journal of Marketing Communications, 24*(1), 68–82.

Peltomäki, J. ja Norppa, K. (2015). *Rikos meni verkkoon: Näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen*. Helsinki: Talentum

Pfleeger, S. ja Caputo, D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers ja Security*, 31(4), 597–611.

Pornpitakpan, C. (2004). The Persuasiveness of Source Credibility: A Critical Review of Five Decades' Evidence. *Journal of Applied Social Psychology*, 34(2), 243–281.

ProCom. Ohjeet ja periaatteet. Saatavilla www-muodossa http://procom.fi/viestintaala/ohjeet-ja-periaatteet/yhteisoviestinnan-periaatteet/ (7.3.2018)

Ries, T. (2017). *Polarization of trust – and implications for business.* Saatavilla www-muodossa https://www.edelman.com/post/the-polarization-of-trust (6.2.2018).

Rydenfelt, H. (2014) Eettinen ennakointi. Toim. Luoma-aho, V. ja Karvonen, E. (2014). *ProComma Academic 2014: Särkymätön viestintä*. Helsinki: ProCom - Viestinnän ammattilaiset ry.

Salman, S., Mat Kiah, M.S., Dhaghighi, B., Hussain, M., Khan, S., Khurram Khan, M. ja Choo, K-K. R. (2016). On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. *Journal of Network and Computer Applications*, 74, 98.

Sarojini, G. (2015). An overview: Trust and reputation in cloud services. *National Journal on Advances in Computing and Management, 6*(2).

Schoorman, F., Mayer, R., ja Davis, J. (2007). An Integrative Model of Organizational Trust: Past, Present, and Future. *The Academy of Management Review,* 32(2), 344–354.

Shin, W., Pang, A. ja Kim, H. J. (2015). Building Relationships Through Integrated Online Media. *Journal of Business and Technical Communication*, 29(2), 184-220.

Slabbert, Y. ja Barker, R. (2014). Towards a new model to describe the organisation–stakeholder relationship-building process: A strategic corporate communication perspective. *Communicatio, 40*(1), 69–97.

Strauβ, N. ja Jonkman, J. (2017). The benefit of issue management: Anticipating crises in the digital age. *Journal of Communication Management, 21*(1), 34-50.

Steyn, B. (2004). From strategy to corporate communication strategy: A conceptualisation. *Journal of Communication Management*, 8(2), 168–183.

Spagnoletti, P., Za, S. ja D'Atri, A. (2007), *Institutional trust and security, new boundaries for virtual enterprises*. International Workshop on Interoperability Solutions to Trust, Security, Policies and QoS for Enhanced Enterprise Systems, Madeira, March 26.

Suomen kyberturvallisuusstrategia (2013). Helsinki: Turvallisuuskomitean sihteeristö. Saatavilla www-muodossa https://jyu.finna.fi/Record/jykdok.1286218 (23.11.2017)

Swanson, R. A. ja Holton, E. F. (2005). *Research in organizations: Foundations and methods of inquiry*. San Francisco, Calif.: Berrett-Koehler.

Syuntyurenko, O. (2015). The digital environment: The trends and risks of development.*Scientific and Technical Information Processing, 42*(1), 24–29.

Telivuo, J. (2015). Rihmasto. Toim. Eriksson, K. (2015). *Verkostot yhteiskuntatutkimuksessa*. [Helsinki]: Gaudeamus.

Thévenot, L. (2007). The Plurality of Cognitive Formats and Engagements: Moving between the Familiar and the Public. *European Journal of Social Theory, 10*(3), 409–423.

Tietosuojavaltuutetun toimiston verkkosivut. EU:n tietosuojauudistus. Saatavilla www-muodossa http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html (12.3.2018)

Tran, M. A., Nguyen B., Melewar, T.C. ja Bodoh, J. (2015). Exploring the corporate image formation process. *Qualitative Market Research: An International Journal*, 18(1), 86–114.

Tuomi, J. ja Sarajärvi, A. (2002). *Laadullinen tutkimus ja sisällönanalyysi*. Helsinki: Tammi.

Tyrväinen, P. ja Selin, J. (2011). *How to Sell SaaS: A Model for Main Factors of Marketing and Selling Software-as-a-Service.* Springer-Verlag.

Vernuccio, M. (2014). Communicating Corporate Brands Through Social Media. *International Journal of Business Communication, 51*(3), 211–233.

Viestintävirasto. (7.9.2017). Verkkotiedote. Verohallinnon nimissä lähetetty tietojenkalasteluviesti. Saatavilla www-muodossa https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/09/ttn201709071144.html (12.11.2017)

Viestintävirasto. (2018). Tietoturvan vuosi 2017. Viestintäviraston julkaisu 001/2018.

Vos, M. (2011). *Integrated communication: Concern, internal and marketing communication* (Fourth edition.). Hague, Netherlands: Eleven International Publishing.

VTT Technical Research Centre of Finland Ltd. (2017). *Improving cybersecurity – How to defend against cyber threats and safeguard operations*. VTT.

Waters, B. (2005). Software as a service: A look at the customer benefits. *Journal of Digital Asset Management, 1*(1), 32.

Wiencierz, C., Pöppel, K. G. and C., Röttger , U. (2015). *Where Does My Money Go? How Online Comments on a Donation Campaign Influence the Perceived Trustworthiness of a Nonprofit Organization*. International Journal of Strategic Communication, 9(2), 102–117

Yle. Ojanperä, S. (6.3.2018). Haittaohjelmahyökkäyksistä myös vaietaan – Lahden kriisistä avoimesti jaettu tieto auttoi muita pysäyttämään WannaMinen. Saatavilla www-muodossa https://yle.fi/uutiset/3-10103405 (25.3.2018)

Yle. (22.11.2017). Uber peitteli 57 miljoonan kuljettajan ja asiakkaan tietojen hakkerointia. Saatavilla www-muodossa https://yle.fi/uutiset/3-9942264 (23.11.2017)

Zerfass ja Viertmann (2017). Creating business value through corporate communication. *Journal of Communication Management, 21*(1), 68–81.

Zhu, D., Lee Z., O'Neal, G. ja Chen Y. (2011). Mr. Risk! Please Trust Me: Trust Antecedents that Increase Online Consumer Purchase Intention. *Journal of Internet Banking and Commerce*, 16(3), 1–23.

Öksüz, A. (2014). Turning Dark into White Clouds – A Framework on Trust Building in Cloud Providers via Websites. AMCIS.

LIITTEET

Liite 1

PITCHAUS ELI MARKKINOINTIKIRJE

Haluatko organisaatiosi menestyvän nyt ja tulevaisuudessa?

Mistä on kyse?

Teen pro gradu -tutkimusta Jyväskylän yliopiston kauppakorkeakoulussa ja tavoitteena on selvittää, miten SaaS-palveluita tuottavat yritykset kokevat voivansa vaikuttaa viestinnällä organisaation maineeseen ja luotettavuuteen digitaalisessa ympäristössä. Lisäksi on tarkoitus selvittää, miten alan organisaatioissa on viestinnässä otettu huomioon alati lisääntyvät kyberturvallisuusuhkat, esimerkiksi haittaohjelmien ja asiakkaiden tietojenkalasteluyritysien lisääntyminen.

Miksi tärkeää?

- verkossa maineen merkitys on korostunut ja korostuu entisestään
- luottamuksella rakennetaan hyvät ja pitkäkestoiset sidosryhmäsuhteet ja luodaan
- turvallisuutta
- kyberturvallisuusuhkat voivat tarkoittaa taloudellisia tappioita ja maineen sekä sidosryhmien menetystä
- aiheeseen liittyvää tutkimusta on tehty vähän

Mitä hyötyä?

- organisaatio saa arvokasta tietoa ja oppia, miten organisaation luotettavuutta voi kehittää
- organisaatio saa tietää, mitä tehdään jo hyvin
- organisaatio saa tietää, missä olisi kehittämisen paikka ja saa halutessaan kehitysehdotuksia
- mahdollisuus benchmarkata muita organisaatioita

Haen haastateltavaksi toimitusjohtajia ja viestinnänammattilaisia, henkilöitä, jotka vastaavat ja hoitavat organisaation viestintää joko oman toimen ohessa tai täysipäiväisesti. Haastattelut tehdään helmikuun lopussa ja heti maaliskuun alussa 2018 puhelinhaastatteluna sinulle parhaiten sopivaan aikaan. Haastatteluun on hyvä varata aikaa reilu 30 minuuttia. Vastaajan henkilöllisyys tai organisaatio eivät tule esille missään tutkimuksen raportointivaiheessa. Haastatteluaineistoa käytetään ainoastaan tähän tutkimukseen eikä sitä luovuteta haastateltavan organisaatiolle tai muille tahoille. Aineisto säilytetään vain tutkimuksen ajan tutkijan toimesta suojaten asiattomilta ja kopioinnilta tai muulta laittomalta käsittelyltä. Raportoinnin jälkeen aineisto hävitetään asianmukaisella tavalla.

Pro gradu -tutkimukseni ohjaa viestinnän johtamisen yliopistonopettaja Outi Ihanainen-Rokio (040 500 8481 / outi.j.ihanainen-rokio@jyu.fi).

Toivon, että kiinnostuit aiheestani ja haluat osallistua tutkimukseni toteutukseen. Otathan minuun yhteyttä joko puhelimitse tai sähköpostilla mahdollisimman pian, jotta voimme sopia ajankohdan haastattelulle. Kiitos!

Ystävällisin terveisin,

Mervi Väisänen
Viestinnän johtamisen maisteriopiskelija
Pro gradun tekijä
Jyväskylän yliopisto kauppakorkeakoulu
mervi.t.vaisanen@student.jyu.fi
050 35 22176

Liite 2

HAASTATTELUKYSYMYKSET

Tervehditään, esittelen itseni ja jutellaan niitä näitä. Sen jälkeen kertaan aiheen, eettisyyden, kerron tutkimuskysymysten määrän, **annan ohjeeksi vastaajan vastata vapaasti + ei ole oikeita tai vääriä vastauksia.** Kerron, että haastateltava voi palata vastaamansa aiheeseen uudestaan, milloin tahansa haastattelun aikana, jos tulee jotain uutta mieleen.

Vastaajan numero:

Taustakysymykset:

1. Mikä on tittelisi organisaatiossa?
2. Teetkö viestintää täysipäiväisesti vai muun työn ohessa? Ajankäyttö?
3. Mikä on viestinnän kokemuksesi vuosissa?
4. Mikä on organisaation henkilöstömäärä?
5. Minkä ikäinen olet?
6. Mikä on sukupuoli?

ANT ja luotettavuus sidosryhmäverkostoissa <u>digitaalisessa ympäristössä</u>

7. Kertoisitko ketkä mielestäsi organisaatiosta viestivät sidosryhmäverkostoissa digitaalisessa ympäristössä?
8. Kuka vastaa organisaation viestinnästä sidosryhmäverkostoissa digitaalisessa ympäristössä?
9. Miten kuvailisit organisaation luotettavuutta digitaalisissa sidosryhmäverkostoissa?
10. Mitkä viestinnälliset tekijät mielestäsi vaikuttavat siihen, että organisaatio koetaan luotettavaksi digitaalisissa sidosryhmäverkostoissa?
11. Kertoisitko, millä tavalla organisaatio mielestäsi tuo viestinnällä esille olevansa rehellinen, tasapuolinen ja oikeudenmukainen digitaalisissa sidosryhmäverkostoissa? Antaisitko esimerkkejä.
12. Miten organisaatio mielestäsi tuo viestinnällä esille noudattavansa lakeja ja muita sääntöjä digitaalisissa sidosryhmäverkostoissa? Antaisitko esimerkkejä.
13. Kertoisitko esimerkkien avulla, millä tavalla organisaatio mielestäsi tuo viestinnällä lisäarvoa sidosryhmille digitaalisissa sidosryhmäverkostoissa?
14. Kertoisitko esimerkkien avulla, millä tavalla organisaatio tuo mielestäsi viestinnällä esille omaa asiantuntijuutta ja osaamista digitaalisissa sidosryhmäverkostoissa?
15. Millä viestinnän tavoilla organisaatio mielestäsi vaikuttaa siihen, että yhteistyö sen kanssa koetaan turvalliseksi digitaalisissa sidosryhmäverkostoissa?

Jos ei tule esille, onko ulkomailla toimintaa ja kuinka laajasti, kysy onko, ja varalta, miten viestitään sinne

Kysyttävä myös mitä digitaalisia sidosryhmäverkostoja organisaatiolla on

Kyberturvallisuusuhkat

16. Luettelen seuraavaksi listan kyberturvallisuusuhkista. Jokaisen mainitun uhkan jälkeen voit sanoa, kyllä, jos se on mielestäsi todennäköistä organisaatiollesi tai ei, jos et pidä sitä todennäköisenä. Saat sanoa niin monta kuin on tarpeen.
    - työntekijöiden ja asiakkaiden tietojen varastaminen
    - verkkokauppa-asiakkaiden luotto- ja pankkikorttitietojen varastaminen
    - yritysvakoilut
    - verkkosivujen, Facebookin, Twitterin jne. tilien kaappaus
    - palvelunestohyökkäykset (verkko kaatuu)
    - haittaohjelmat organisaation laitteisiin
    - SMS huijausviestit organisaation nimissä
    - sähköpostit organisaation nimissä
    - ansasivustot (organisaation verkkosivujen päällä, linkkinä sähköpostissa)
    - verohuijaus
    - valeverkkokauppa
    - Microsoft Office tai muun tunnetun ohjelman nimissä tapahtuva tietojen kalastelu
    - organisaation oman ohjelman nimissä tapahtuva tietojen kalastelu
    - tuleeko mieleesi jotain muuta, mikä?

17. Mikä voisi mielestäsi olla pahin mahdollinen seuraus organisaatiolle, joka voisi tapahtua uhkan toteutuessa?
18. Millä tavalla edellä mainitut uhkat on otettu huomioon organisaation viestinnässä digitaalisessa ympäristössä?
19. Miten uhkat mielestäsi tulisi ottaa huomioon organisaation viestinnässä digitaalisessa ympäristössä?

Muut kysymykset

20. Tuleeko mieleesi muuta, jota haluaisit sanoa keskustelemiimme asioihin liittyen?
21. Haluatko saada valmiin lopputyön itsellesi:
    Kylläsähköpostisosoite
    Ei
22. Miltä haastattelu sinusta tuntui?

Kertaan, mitä nyt tapahtuu, eettisyyden ja missä vaiheessa organisaatioon otetaan yhteyttä.

Kiitän osallistumisesta haastatteluun.

Liite 3

Ote Lild -kauppaketjun kotisivuilta 12.1.2018 koskien WhatsUp huijausviestiä.