”KYLLÄ MÄ NIINKU AIKA HOUSUT KINTUISSA OLISIN JOS JOTAIN TULISI” – SUOMALAISTEN JOURNALISTIEN KOKEMUKSIA TOIMITUSTYÖN TIETOTURVASTA

Petri Markkanen
Maisterintutkielma
Journalistiikka
Kieli- ja viestintätieteiden laitos
Jyväskylän yliopisto
Kevät 2022

JYVÄSKYLÄN YLIOPISTO

Tiedekunta Humanistis-yhteiskuntatieteellinen	Laitos Kieli- ja viestintätieteiden laitos
Tekijä Petri Markkanen	
Työn nimi ”Kyllä mä niinku aika housut kintuissa olisin jos jotain tulisi” – Suomalaisten journalistien kokemuksia toimitustyön tietoturvasta	
Oppiaine Journalistiikka	Työn laji Maisterintutkielma
Aika Kevät 2022	Sivumäärä 44+1

Tiivistelmä

Miten tietoturva näkyy toimittajan arkityössä, entä millaisia tietoturvaan liittyviä uhkia toimittajat kokevat työssään? Tässä maisterintutkielmassa paneudutaan journalismin ja tietoturvan monimutkaiseen suhteeseen haastattelemalla kotimaisia toimittajia heidän kokemuksistaan tietoturvasta ja sen riskeistä. Tutkimuksen tavoitteena oli koota rivitoimittajien kokemuksia aiheesta tutkimusta varten ja peilata aktiivisessa kansainvälisessä tutkimuksissa ilmenneisiin havaintoihin.

Tutkimus toteutettiin keväällä 2022 haastattelemalla neljää suomalaisessa mediatalossa työskentelevää toimittajaa. Aineisto kerättiin puolistrukturoidun haastattelun keinoin ja analysoitiin temaattista sisällönanalyysia käyttäen. Aineistossa ja analyysissa kuullaan toimittajien omaa käsitystä uhkakuvista ja ongelmatilanteista, mutta myös ratkaisuehdotuksista ja kehittämistoiveista. Työantaja saa kriittisen roolin monen haastateltavan suulla: tietoturva ei työntekijän silmin tarkoita vain valmiiksi asennettua työkonetta tai intranetin syövereistä löytyviä ohjeita. Ala kaipaisi tulosten perusteella asennemuutoksen lisäksi selkeämpiä tietoturvaa parantavia toimintamalleja sekä yhteisiä pelisääntöjä. Tutkimusaineisto pitää sisällään huolta, mutta myös toivoa: tietoturvasta puhuminen on yleistynyt toimituksissa ja toimittajat ovat itse pohtineet ratkaisuja käytännön ongelmatilanteisiin

Tulosten perusteella suurimpina ongelmina toimittajat kokevat tietoturvallisuuden abstraktiuden, osaamattomuuden kokemukset ja lähdesuojan kaksisuuntaisuuden haasteet. Työnantajan ristiriitaisuus tietoturvan priorisoinnissa herättää arvokasta keskustelua, samoin tietoturvauhkien tunnistamisen haasteet. Se, miten journalismia tulevaisuudessa tehdään entistä turvattomammassa verkkomaailmassa, on kiinni sekä tekijöistä että johtoportaasta.

Asiasanat: Journalismi, kyberuhka, tietoturva, tietoturvallisuus, tietoturvauhka, kyberturvallisuus

Säilytyspaikka: Jyväskylän yliopisto

Muita tietoja

SISÄLLYS

1 JOHDANTO

2010- ja 2020-lukujen uutisointia värittivät Edward Snowdenin tietovuotojen kaltaiset mediailmiöt, Psykoterapiakeskus Vastaamon tietomurto ja Puolustusvoimien Viestikoekeskuksen uutisointi ja sen myötä toimittajan kotiin tehty kotietsintä. Tätä johdantoa kirjoittaessa Eurooppaan on syttynyt sota. Venäjän helmikuinen hyökkäys Ukrainaan on nostanut informaatiovaikuttamisen lisäksi kyberhyökkäysten riskit suomalaistenkin arkeen ja työelämään.

Journalisti ei ole turvassa vaikuttamisyrityksiltä tai kyberuhilta, kuten tietojen kalastelulta, hakkeroinnilta tai häirinnältä. Toimittaja käsittelee työssään arkaluontoista tietoa ja on tietoturvallisesti hyvin kiinnostava kohde. Hänellä on tietoa, jota muilla ei ole, sekä kykyä ja kanava vaikuttaa asioihin (Watkins ym., 2017). Toimitusten kirjavat organisaatiomallit, toimittajien vaihtelevat työsuhdetyypit ja verrattain autonominen työ vastuineen vaikuttavat siihen, miten eri tavoin journalismi on haavoittuvainen tietouhkille (Crete-Nishihata ym., 2020). Journalismin tutkimuksessa esille nousee luonnollisesti lähdesuojan turvaaminen, jossa ongelmakohdiksi ovat nousseet esimerkiksi toimittajien osin välinpitämätön suhtautuminen lähteen haavoittuvuuteen (Bradshaw, 2017) ja teknologisen ymmärryksen puutteet niin lähteillä kuin toimittajilla (Lee & Heinrichs, 2019).

Toimituksissa alati kehittyvään teknologiaan ja sen tietoturvallisuusvaikutuksiin on reagoitu vuosien varrella kirjavasti. Osassa toimituksia on ollut nähtävissä nihkeyttä uusia tietoturvametodeja kohtaan (Watkins ym., 2017), kun taas esimerkiksi Yhdysvalloissa Tor-verkossa toimiva SecureDrop-viestiväline on osoittautunut kullanarvoiseksi paljastuksentekijöiden apuna (Di Salvo, 2021). Turvallisen viestintätavan mahdollistaminen tuli tärkeäksi viimeistään presidentti Donald Trumpin valtakaudella, kun yhdysvaltalaistoimitukset ottivat hallituksen virkailijoilta vastaan tietovuotoja ja paljastuksia.

Toimittajakunta joutuu valitettavan usein olemaan valtiovallan ja tiedusteluelinten tarkkailun kohteena eikä tietomurtoja voi aina ennakoida edes ajantasaisilla välineillä

tai osaamisella. Viime vuonna liki 200 journalistia maailmanluokan toimituksista yhdessä tuhansien ihmisoikeusaktivistien ja juristien kanssa oli joutunut massiivisen valtiotason tietohyökkäyksen kohteeksi. Kyseessä oli israelilaisen tiedusteluyrityksen haittaohjelma Pegasus, jota myös Unkarin Viktor Orbánin johtaman hallinnon väitetään käyttäneen maansa tutkivia toimittajia vastaan (Kirchgaessner ym., 2021). Tämä on vain yksi esimerkki monista, mutta huolestuttava sellainen.

Tutkimusaiheena journalistien tietoturva on Suomessa kuitenkin uusi kokonaisuus. Maassamme ei olla julkisesti tutkittu toimitusten tietoturvaa yleisemmälläkään tasolla. Kyberturvallisuutta tutkitaan yliopistoissa informaatioteknologian tieteenalalla esimerkiksi asiantuntijaorganisaatioiden osalta, mutta toimitusten ja erityisesti rivitoimittajien osalta tutkimuksessa on käytännössä kotimaan kokoinen aukko. Kansainvälisesti taas journalismin ja tietoturvan suhde on ollut pöydällä vähintään vuosikymmenen ajan kuitenkin keskittyen lähinnä länsimaihin, kuten Yhdysvaltoihin ja muuhun anglosaksiseen maailmaan. Yksi merkittävimmistä lähtösysäyksistä tutkimukselle oli vuoden 2013 Edward Snowdenin tekemät tietovuodot medialle. Tapahtuman seurauksena erityisesti lähdesuojan murtumattomuuden lupaus ja toimittajien rooli valtiotasojen tietojenkeruun paineissa nousi keskustelun ja tutkimuksen keskiöön (esim. Bradshaw, 2017; Lashmar, 2017; Wahl-Jorgensen ym., 2017).

Henkilökohtainen kiinnostukseni tietoturvaa kohtaan kumpuaa suurelta osin siitä, mitä olen nähnyt toimittajan urallani ja toisaalta kuullut eri toimituksissa työskenteleviltä kollegoiltani. Tietoturvakäytännöt vaihtelevat aivan kuin työolot ja työsuhteetkin. Vaikka omissa kokemuksissani ei juuri ole negatiivista sanottavaa, osa kollegoideni kertomasta on saanut kulmat kurtistumaan – voidaanko tätä luottamukseen perustuvaa työtä tehdä niin, että vaarannetaan jopa lähteen turvallisuus? Muun muassa tähän kysymykseen lähdin etsimään vastausta tätä tutkimusta suunnitellessani.

Tutkimukseni aihe on vähintäänkin arkaluonteinen. Väitän, että se on osin, ellei kokonaan, tabu. Tietoturvaongelmista ei ole ollut tapana puhua julkisesti. Tämä on ymmärrettävää aiheen itsensä vuoksi. Mikään taho tuskin haluaa vapaaehtoisesti paljastaa digitaalisia tai fyysisiä haavoittuvuuksiaan. Tietoturva ei ole myöskään nauttinut mediaseksikkäimmän otsikon tittelistä vasta kuin viime vuosina, ja tästäkin kiitos kuuluu kriiseille ja konflikteille, oli kyse sitten tietomurrosta tai sodasta. Digitaalisesta turvallisuudesta on tullut pop, koski se sitten journalistisen työprosessin suojelua, julkisen organisaation toimintavarmuutta tai yksittäisen ihmisen verkkokauppaostoksen maksamista.

Kotimaisen tutkimuksellisen tyhjiön, kansainvälisesti aktiivisen tutkimuksen ja omakohtaisen kiinnostukseni tuloksena olen määritellyt tutkimusongelmaksi seuraavan: *miten suomalaiset toimittajat kokevat tietoturvan ja mahdolliset tietoturvauhat työssään*.

Tutkimuskysymykset:

1. Miten toimittajat kokevat tietoturvallisuuden osana työtään?
2. Millaisia tietoturvauhkia toimittajat mahdollisesti kokevat työssään?

Ensimmäisen tutkimuskysymyksen avulla haen vastauksia siihen, millä tavalla suomalaiset toimittajat kokevat tietoturvallisuuden työssään. Toinen tutkimuskysymys käsittelee mahdollisia tietoturvaan liittyviä uhkia, joita haastateltavat ovat kokeneet tai uskovat kokevansa työssään. Vastauksia tutkimuskysymyksiin haetaan haastattelun keinoin neljältä suomalaiselta toimittajalta, joiden identiteetti on tutkimuksessa anonymisoitu henkilöllisyyden suojaamiseksi. Tunnistettavuuden häivyttäminen oli yksi työn onnistumisen elinehto.

Tavoitteenani on, että tutkimukseni anti pääsisi hyötykäyttöön ruohonjuuritasolle, sinne, missä journalismin kenttätyötä tehdään. Haastatteluista kaivettujen tulosten tärkein anti on niissä pohdinnoissa ja mietteissä, joista ei toimituksen kahvipöydässä tai kehityskeskusteluissa juuri hiiskuta. Tutkimukseni henkilökohtainen tavoite on saavutettu, jos yksikin toimittaja – tai lähde – muuttaa tietoturvakäytäntöjään turvallisempaan suuntaan.

Tiedostan, että tutkimukseni raapaisee vain pintaa suomalaisesta journalismin kentästä. Jatkotutkimus tulee toivottavasti pureutumaan syvemmälle ja monipuolisemmin aiheeseen. Tarvetta sille – ja tietoturvan parantamiselle – journalismissa on. Se, onko neljä haastateltavaa riittävästi vastaamaan koko suomalaisen mediakentän puolesta, jakaa todennäköisesti mielipiteitä. Tätä tutkimusta varten tuo määrä haastateltavia on riittävä ja toivonkin, että tulevaisuudessa näen tutkimuksia suuremmalla vastaajamäärällä. Kuten sanottua, tämä on vain pintaraapaisu. Näen aiheen tutkimuksen tulevaisuuden valoisana, sillä koen, että tämän tutkimuksen myötä jatkotutkimukselle on jo saatu alan sosiaalinen hyväksyntä.

Journalistisen kulttuurin edistämissäätiö JOKES myönsi 2 000 euron apurahan tämän tutkimuksen viimeistelyyn.

2 AIEMPI TUTKIMUS

Tässä luvussa esittelen ensimmäisen alaluvun osalta journalismia ja tietoturvaa koskevaa aiempaa tutkimusta journalismin, informaatioteknologian ja kyberturvallisuuden tieteenaloilta. Toinen alaluku käsittelee lähdesuojan ja tietoturvan suhdetta. Viimeisessä alaluvussa käyn läpi tutkimusta, joka koskee toimittajia koskevia tietoturvauhkia. Käytännössä kaikki tutkimus on kansainvälistä ja keskittyy pääosin länsimaisesta näkökulmasta tutkittuihin ilmiöihin ja tapauksiin. Jokaisessa alaluvussa käsittelen lyhyesti myös aiheisiin kuuluvat keskeisimmät käsitteet.

2.1 Journalismi ja tietoturva

Journalismin tietoturvaa on tutkittu maailmalla aktiivisesti erityisesti 2010-luvulta asti. Tietoturvaan, joka pitää sisällään fyysisen ja digitaalisen maailman tietosuojan, on usein yhdistetty kyber-alkuiset, digitaaliseen ympäristöön liittyvät uhkat, kuten kyberturvallisuus ja kyberuhkat. Suomen valtion Liikenne- ja viestintävirasto Traficomin alaisen Kyberturvallisuuskeskuksen (2022) mukaan tietoturva koostuu hallinnollisista ja teknisistä toimista, joilla varmistetaan, että vain käyttöön oikeutetuilla on mahdollisuus käyttää turvattua tietoa eikä tietoja voi muuttaa kuin vain siihen oikeutetut tahot. Käytännössä tämä määritelmä tarkoittaa sitä, että oikeilla välineillä ja päätöksillä varmistetaan, että kukaan ulkopuolinen ei pääse käsiksi tietoon. Tietoturvan ja kyberturvallisuuden termien välillä on eroja. Tietoturva pitää sisällään ne tekijät, jotka edistävät tietosuojaa, kuten yksityisyydensuojaa, kun taas kyberturvallisuus liittyy kiinteästi digitaalisen maailman turvallisuuteen. Janssonin ja Sihvosen (2018) määritelmän mukaan kyberturvallisuus pitää sisällään yhteiskunnallisen tason tietoliikenne- ja viestintäjärjestelmien toimivuuden ja turvaamisen – teknologisen puolen lisäksi termi pitää sisällään siis poliittisen

ulottuvuuden. Oman haasteensa tulkintaviidakkoon tuo se, että ulkomaisessa tutkimuksessa esiintyy termeistä sekä tietoturvaa (information security) että kyberturvallisuutta (cybersecurity). Tässä tutkimuksessa käytetään pääasiassa termiä tietoturva, joka kattaa laajemmin myös yksityisyydensuojan.

Journalismin ja tietoturvan suhde ei kuitenkaan ole millään tavalla yksinkertainen tai suoraviivainen. Päätutkimussuuntia on tämänhetkisessä tutkimuksessa melko selväpiirteisinä kaksi. Philip Di Salvon (2022) määritelmän mukaan ensimmäinen teema käsittelee tietoturvaan liittyviä työkaluja ja käytäntöjä sidottuna journalistiseen kontekstiin. Toinen teema taas keskittyy tietoturvaan liittyviin motiiveihin, perusteisiin ja organisaatioihin liittyviin haasteisiin, joita tarkastellaan journalistisesta näkökulmasta. Suuntausten rajat eivät ole tarkkarajaisia, mutta eron voisi selvimmin kiteyttää seuraavasti: ensimmäinen tutkii enemmän välineellistä tietoturvaa ja toinen taas kulttuurista tietoturvaa. Kulttuuriseen tietoturvaan liittyy olennaisesti myös toimittajien asenteet ja käytösmallit. Varsinaisen kaksinapaisen määritelmän ulkopuolellakin on tutkimusta ja yksi vähemmän tutkittu aihepiiri on omaa tutkimustanikin koskeva toimittajien kokema digitaalinen häirintä, jonka Di Salvo on nostanut vakavimmaksi uhaksi yhdessä valtiotahojen tiedustelun ja vakoilun jälkeen, josta toimittajat myös kärsivät (Di Salvo, 2022).

Journalistisen työn ja tietoturvan suhde on vähintäänkin monimutkainen ja aina kontekstista riippuvainen. Yksi teemaa selventävä määritelmä liittyy kiinteästi työkulttuuriin ja toimittajien käytökseen: ei ole olemassa yhtä yksittäistä journalistista tietoturvakulttuuria, vaan alalla on kokonainen kulttuurien kirjo muuttujineen (Crete-Nishihata ym. 2020). Tähän moninaisuuteen vaikuttavat erilaiset arvot, uutistyön teon tavat sekä uutissisällön ulosanti. Yksi tietoturvakulttuuriin liittyvä havainto on se, että jutun ja lähteen tärkeäksi kokeminen vaikuttavat siihen, ajatteleeko journalisti tietoturvallisuuden tärkeäksi työn kannalta. Crete-Nishihatan ym. (2020) Kanadassa tekemän tutkimuksen perusteella esimerkiksi tutkivat journalistit kokevat valtiotiedustelun uhkaavampana kuin perinteistä journalismia tekevät. Voidaankin puhua ilmiöstä, jossa journalistit ajattelevat, että tietoturva ei kosketa heitä. Vastaavasta ilmiöstä havainnon tehneet Susan McGregor ja Elizabeth Watkins (2016) käyttivät tutkimuksessaan mielikuvamalleja selittämään journalistien tietoturvakäytöstä- ja asenteita. Security by obscurity-mallin mukaan journalistit kokevat tietoturvan tärkeänä vain, jos he työskentelevät valtiotason tai yhteiskunnallisten aiheiden parissa. Tämä kertoo myös olettamuksesta, että toimittajien tietoturvakäytös perustuisi ainakin joltain osin työnkuvaan (McGregor & Watkins, 2016). Vaikutusta näyttäisi olevan myös sillä, onko toimittaja kiinni organisaatiossa, ts. vakituisessa työsuhteessa vai freelancer – jälkimmäisillä on

enemmän vapautta työssään, mutta selvästi vähemmän resursseja tietoturvan ylläpidossa tai kehittämisessä. Viitteitä on myös siitä, että organisaatiossa työskentelevät journalistit eivät saa mielestään ääntään kuuluviin, vaikka he haluaisivat parantaa työnsä tietoturvaa – tämä johtuu johdon ja toimittajien erilaisista prioriteeteista ja on jopa johtanut siihen, että yksittäiset toimittajat toimivat omin päin tietoturvaa parantaakseen (Crete-Nishihata ym. 2020). Yksi tämän ”kuilun” syy liittyy todennäköisesti organisaatiokulttuuriin itsessään: McGregorin ym. (2016) mukaan haastatteluissa on selvinnyt, että yksittäisten toimittajien ja toimitusorganisaation, tarkemmin yrityksen johtoportaan, välillä vallitsee usein yhteisymmärrys tietoturvan tärkeydestä, mutta uhkien priorisoinnissa ja yksityisyydensuojassa tahot ovat omissa leireissään. Toimittajat keskittyvät arjen työssään pääasiassa tiedonhankintaan ja lähdesuojan pitävyys on monesti kiinni myös lähteen tietoturvaosaamisesta eikä niinkään toimitusorganisaation omasta toiminnasta. Oman haasteensa tuo sekin, että yhtiötasolla mediataloissa keskitytään sisäiseen turvallisuuteen laajemmassa skaalassa, esimerkiksi toimittajien suojaamiseen tietojenkalastelulta (McGregor ym, 2016). Vaikka journalistista tietoturvakulttuuria on tutkittu maailmalla, Suomessa aihe ei ole herättänyt juurikaan julkista keskustelua. Tietoturvakulttuureihin ja myös asenteisiin nähden olisi aiheellista tutkia, millä tavoin suomalaiset toimittajat kokevat tietoturvan päivittäisessä työssään ja onko esimerkiksi toimittajan työroolin tyypillä tai yrityksen johtamismalleilla merkitystä siihen, millä tavalla tietoturvaan ja lähdesuojaan suhtaudutaan.

Suhtautumistapoja ja omia käytösmalleja on onneksi mahdollista muuttaa. Ymmärrys siitä, että työskentelee tietoturvaa vaativassa ympäristössä voi auttaa parantamaan omaa turvallisuutta muuttamalla ajattelumalleja. Hongkongilaisten journalistien turvallisuusajattelua ja sen malleja tutkineet Lokman Tsui ja Francis Lee (2021) katsovat, että journalistien parempi käsitys tietoturvauhista tekee esimerkiksi kollegoiden ja lähteiden kanssa viestimisestä turvallisempaa. Tähän muutokseen vaikuttaa riskien ja uhkien ymmärtäminen, johon liittyy vahvasti se, tekeekö toimittaja tutkivaa journalismia vai ei. Tutkivilla toimittajilla on nimittäin parempi ymmärrys digitaalisista uhkista, vakoilun kohteeksi joutumisesta ja oikeustoimilla uhkailusta. Positiivisena seurauksena ymmärryksen laajenemisesta koituu se, että hyvällä tolalla oleva tietoturva ja ymmärrys sen tärkeydestä auttaa toimittajia myös tarttumaan muun muassa poliittisesti ja yhteiskunnallisesti herkempiin juttuaiheisiin. Journalistien välillä on kriittisiä eroja nimenomaan ajattelumalleissa: esimerkiksi ne hongkongilaistoimittajat, jotka työskentelevät ainakin osin Manner-Kiinassa, omaavat paremmat tietoturvataidot sekä ymmärryksen valtiolähtöisestä valvonnasta työtään kohtaan. Työn lokaatio ja se, missä kulttuurissa työskennellään, voi siis tuoda muutoksia tietoturva-ajatteluun ja tietoturvakäytäntöihin (Lokman & Lee, 2021).

Suomessa vastaavan kaltaisia ajatusmalleja toimittajien keskuudessa ei ole vielä tutkittu. Lehdistönvapaus on Suomessa maailman kärkikastia ja oman tutkimukseni kannalta on tärkeää tarkastella, tuleeko sananvapauden teema esiin tietoturvakontekstissa ja jos, missä muodossa.

Vaikka toimitustyön voisi universaalisti kuvitella elävän tarkasti alan normien mukaisesti, (tieto)turvallisuus vaikuttaa olevan enemmänkin yksilöllinen kuin yhteisöllinen haaste (Henrichsen, 2021). Käytännössä tämä tarkoittaa sitä, että toimituksissa ei aina ymmärretä tietoturvan olevan ”kaikkien asia”. Ne toimittajat, jotka ovat paneutuneita tietoturvaan sekä valmiita muuttamaan käytäntöjä paremmiksi, eivät saa muutoksia aikaan. Tämä johtuu siitä, etteivät nämä ”tietoturvan esitaistelijoiksi” kutsutut toimittajat ole siinä statuksessa, että voisivat muuttaa käytännön työtä (Henrichsen, 2021, s. 14). Vastaava havainto peilautuu myös jo aiemmin mainitusta Crete-Nishihatan ym. (2020) tutkimuksesta – voidaan siis todeta, että tarpeeksi korkean työstatuksen puuttuminen vaikeuttaa muutosten tekemistä työyhteisössä. Tämä on luonnollista, mutta tietenkin harmillista yhteisön tietoturvakehityksen kannalta. Kuitenkin näillä tietoturvaan perehtyneillä toimittajilla on tärkeä rooli työyhteisöissä: he ovat usein niitä, jotka auttavat kollegoita ja jakavat avoimesti tietoa paremman työyhteisön puolesta. Elizabeth Watkins ja C. W. Anderson (2019) ehdottavat tähän yhdeksi ratkaisuksi mahdollisimman monipuolisen ja taidoiltaan toisistaan risteävän toimittajajoukon kokoamista (Watkins & Anderson, 2019). Toimittaminen on loppujen lopuksi jutunteon nopeuskilpailu ja voikin sanoa tietotekniikan olevan joissain tapauksissa jarru tiedon nopeassa välittämisessä – ainakin, jos puhutaan tietoturvallisesta viestimisestä, jossa useita ohjelmia ketjutetaan tai kirjautumisia järjestelmiin pitää hyväksyttää useaan kertaan.

Mitä tietoturva journalistisessa kontekstissa sitten pitää sisällään? Di Salvo (2022) tekee jaottelun kulttuuriseen ja välineelliseen tietoturvaan – asenteiden, koulutuksen ja taitojen rinnalla kulkevat teknologiset ratkaisut, kuten työssä käytetyt laitteet ja niiden ohjelmistot aina puhelimista tietokoneisiin. Journalistien käyttämiä salaavia ohjelmistoja tutkinut Di Salvo (2021) toteaa journalismin tietoturvavälineiden- ja -käytänteiden tutkimuksen olevan vasta aluillaan, mutta jo nyt on selvinnyt, että uutistoimituksissa on heräävää kiinnostusta tietoturvaratkaisuihin ja teknologioihin, kun ne koskevat lähteen suojaamista. Tämä on osin ristiriitaista, mutta myös helpottavaa aiempaan tutkimukseen nähden: journalistisen tietoturvan puutteista on kritisoitu jo Edward Snowdenin vuoden 2013 tietovuotojen jälkeen, joten tuoreen tutkimuksen tulokset voivat kieliä siitä, että asenteet ovat vihdoin muuttumassa. Kuitenkin tänä päivänä toimituksilla on kiinnostusta teknologioihin, kuten

SecureDropiin, journalisteille ja tietolähteille luotuun avoimen lähdekoodin ohjelmaan, jonka avulla lähde pystyy kommunikoimaan, kuten lähettämään tiedostoja, anonyymisti salattua Tor-verkkoa käyttäen. Haasteen tuo kuitenkin mahdollisuus siitä, että SecureDrop koetaan jopa liian turvalliseksi lähteiden silmissä, jolloin sen ylimitoitettu käyttö voisi pelottaa lähteitä pois. Kyseessä olisi siis liiallisen turvallisuuden mainostaminen, joka voisi laukaista eräänlaista paniikkireaktiota lähteissä (Di Salvo, 2021). Mielenkiintoista on se, että vaikka SecureDrop on ollut markkinoilla tutkimuksen kirjoitushetkellä jo kahdeksan vuotta, se on käytössä vain pääasiassa suurissa länsimedioissa ja vieläpä erityisesti Yhdysvalloissa. Esimerkiksi Suomessa SecureDropia tai sen kaltaista suojattua ”pilliinviheltäjälinjaa” ei käytä mikään media, ainakaan vielä.

Tietotyön teknologian turvallisuuteen liittyy harmaa osa-alue, jota kutsutaan englanniksi termillä Shadow IT. Tässä tutkimuksessa käytän siitä vapaasti suomennettua versiota varjo-IT, jota näkee käytettävän myös teknologiaan painottuvassa uutisoinnissa ja näin suomennettu termi on perusteltu tähän työhön. Kiteytettynä termi tarkoittaa esimerkiksi sitä, että työntekijä tekee työtehtäviään sellaisilla välineillä, ohjelmistoilla tai palveluilla jotka eivät ole hyväksyttyjä tai tiedostettuja yrityksessä (Rentrop & Zimmermann, 2012). Varjo-IT ei kuitenkaan lähtökohtaisesti ole pahantahtoisen tarkoitusperän lopputulos, vaikka vaikutukset voivatkin olla tietoturvallisesti negatiivisia. Steffi Haag ja Andreas Eckhardt (2014) taas määrittelevät varjo-IT:n ilmiönä, jossa työntekijä käyttää mitä tahansa työpaikan sääntöjä rikkovaa it-resurssia parantaakseen työtehokkuuttaan – ja kuten sanottua, kuitenkaan ilman tarkoitusta vahingoittaa organisaatiota. Käytännössä siis työntekijä tekee töitä omin päin välineillä, joista työnantaja ei tiedä. (Haag & Eckhardt, 2014). Riskit tietoturvalle syntyvät molemmissa edellä mainituissa tapauksissa yksinkertaisesti siitä, ettei työnantaja tai organisaatio pysty tarjoamaan tarpeellista tietoturvaa laite- ja ohjelmistokontrollin puuttuessa. Journalismissa varjo-IT muodostuu ongelmalliseksi sen moninaisuuden ja arkaluonteisuuden vuoksi: käyttävätkö toimittajat omia välineitä, ymmärtävätkö he tekevänsä väärin ja jos, uskalletaanko käytännöstä puhua. Toimittajat tekevät luottamuksellista työtä ja työelämä vaatii jatkuvaa tehostamista – on aivan mahdollista, että tehokkuutta haetaan tuttujen välineiden tai ohjelmistojen kautta välittämättä tai tietämättä niiden tietoturvasta. Arkaluontoista on se informaatio, joka on vaarana paljastua varjo-IT:n käytön myötä: jos oletetaan, että tietoturvaa ei henkilökohtaisissa laitteissa käytetä, riski tietomurrolle on huomattavasti suurempi kuin työvälineellä, jossa tietoturva on kunnossa organisaation toteuttamana. Varjo-IT on tutkimuksessa kuitenkin varsin uusi aihepiiri ja sen määrittely osin vielä lapsenkengissään. Sitä määritellään teknologian tai työnteon konkretian kautta, osin taas ihmisen käytösmallien kautta.

Jaottelussa voi nähdä samoja piirteitä kuin Di Salvon (2022) tietoturvajaottelussa välineellisestä ja kulttuurisesta tietoturvasta. Aihe tarvitsee selvästi lisää tutkimusta niin informaatioteknologian puolella kuin myös journalistisessa kontekstissa. Tässä tutkimuksessa varjo-IT ei ole pääosassa, mutta kuitenkin sen verran merkittävässä roolissa, että sen avaaminen näin laajasti on perusteltua. Tämän työn aineistoanalyysissa ja pohdinnoissa paneudutaan sekä tekniseen että henkiseen puoleen varjo-IT:n osalta kuitenkaan menemättä syvällisesti psykologisiin tulkintoihin.

2.2 Lähdesuoja ja tietoturva

Tässä alaluvussa käsittelen lähdesuojan ja tietoturvan suhdetta. Tutkimukseni kannalta lähdesuojan aiempaa tutkimusta on tärkeä avata syvällisemmin, koska lähdesuoja on journalismin kannalta kriittinen sekä haavoittuva kohde ja toimittajat ovat viime kädessä vastuussa siitä, ettei toimittajaan luottavan tietolähteen henkilöllisyys paljastu. Aiemman tutkimuksen mukaan toimittajien suhtautumisessa lähdesuojan tietoturvaan on eroavaisuuksia.

Lähdesuojan tarkoitus on suojella lähdettä, joka on paljastanut toimittajalle arkaluontoisia tietoja. Maarit Jaakkolan (2013) mukaan toimittajan lähteelleen antama lähdesuoja tarkoittaa sitä, että toimittaja ei esimerkiksi paljasta viranomaisille arkaluontoisten tai epäkohtia paljastaneen henkilön henkilöllisyyttä. Lähdesuoja perustuu Suomen lakiin (Laki sananvapauden käyttämisestä joukkoviestinnässä, 16 §) ja sillä pyritään takaamaan sananvapauden toteutuminen yhteiskunnassa. Lähdesuoja voidaan nähdä myös toimittajan luottamuksen mittarina: journalistilla on velvollisuus pitää luottamuksellisia tietoja antaneen lähteen henkilöllisyys salassa. Yleisesti lähteen paljastumista ei pidetä suotavana tai hyväksyttävänä. Vasta oikeus voi Suomessa murtaa lähdesuojan tilanteessa, jossa syyttäjä vaatii jollekulle rangaistusta. (Jaakkola, 2013).

Kuten jo aiemmassa luvussa avatusta tutkimustiedosta voi todeta, suhtautuminen lähdesuojaan ja sen haavoittuvuuteen toimituksissa vaihtelee. Lisäksi lähdesuoja ja teknologia kävelevät tutkimuskentällä melkein käsi kädessä, onhan teknologia yksi tärkeimmistä kommunikaation mahdollistajista. Teknologisen kehityksen perässä pysyminen on monelle kuitenkin vaikeaa eivätkä journalistit eroa tässä muista ihmisistä. Henrichsenin (2020) tuoreen tutkimuksen mukaan voidaan jopa sanoa, että journalistit ja toimitukset itse ovat joissain tapauksissa uusien välineiden käyttöönoton suurimpia jarruja. Vaikka journalismin tekijöiden ja alan kuvittelisi

olevan uusien tietoturvallisten metodien edelläkävijöitä, journalistien suhtautumista ja kykyjä ottaa käyttöön uusia tietoturvallisia teknologioita leimaa omalaatuinen nihkeys, joka kumpuaa riskien ymmärryksen puutteesta. Henrichsenin (2020) tutkimuksesta käy ilmi, että toimittajaa ja juttua (engl. story) suojellaan, mutta lähdesuoja jää paikoin olemattomaksi. Lisäksi ongelmia tuovat toimittajien usko siihen, että tietoturvakulttuuria tarvittaisiin vain valtiotason asioita tutkiessa. Havainto on samansuuntainen kuin Crete-Nishihatan ym. (2020) ja MgGregorin ja Watkinsin (2016) tutkimuksissa. Hälyttävänä esimerkkinä tutkimuksessaan Henrichsen (2020) nostaa kuitenkin sen, kuinka vähän tutkimuksessa mukana olleet yhdysvaltalaistoimittajat nostivat lähdesuojan roolia esiin tietoturvallisen työskentelyn kontekstissa. Toimittaja voi esimerkiksi olla hyvinkin valmis suojelemaan työrooliaan ja juttuansa kyberuhilta, mutta ajatus siitä, että journalistin olisi suositeltavaa ottaa käyttöön digitaalisia tietoturvateknologioita lähdettä suojellakseen, loisti poissaolollaan (Henrichsen, 2020). Lisäksi aiemmassa tutkimuksessa on ilmennyt, ettei lähdesuoja ole yhtä korkealla kaikkien toimittajien arvomaailmassa. Paul Bradshaw (2017) tutki Edward Snowdenin vuoden 2013 tietovuotojen jälkeistä Ison-Britannian paikallismedioita ja tuli tulokseen, ettei paikallismediakentällä suhtauduta tarpeeksi vakavasti lähdesuojan parantamiseen tai teknologisiin uhkiin, vaikka mediaa mullistaneesta Snowdenin tapauksesta oli kulunut jo vuosia. Oli jopa niin, että tutkimukseen haastatelluilla toimittajilla esiintyi välinpitämättömyyttä sitä kohtaan, miten heidän työnantajansa suojaa työntekijöitään ja toimitustyötä: melkein joka kolmas tutkimukseen osallistunut uskoi työantajansa ”tehneen tarpeeksi” journalistiensa suojaamiseksi – tämä väite tosin perustui vain toimittajien omiin oletuksiin tietoturvan ja tietosuojan tasosta (Bradshaw, 2017). Bradshaw’n tutkimus koskettaa tämän tutkimuksen aihetta läheisesti, sillä sen kautta tarjoutuu mahdollisuus tarkastella suomalaisesta näkökulmasta sitä, miten toimittajat kokevat työantajan roolin tietoturva-asioiden kehittämisessä ja lähteiden suojaamisessa. Luotettavien lähteiden (engl. confidential source) lähdesuojaa tutkineen Paul Lashmarin (2017) mukaan on selvää, että turvallista digitaalista kommunikaatiota ei ole olemassa ja journalistien olisi syytä tiedostaa tämä. Lashmarin tutkimukseen haastateltujen kahdentoista toimittajan suurimpina huolenaiheina olivat valtiotason valvonnasta johtuva uhka, joka kohdistui lähdesuojaan: toimittajat eivät välttämättä pysty lupaamaan täydellistä lähdesuojaa valvonnasta johtuen. Tästä voi olla negatiivisia vaikutuksia siihen, miten toimittajia uskalletaan lähestyä hyvin arkaluontoisten juttuaiheiden tai tietojen kanssa (Lashmar, 2017). Vaikka Lashmar käsitteleekin tutkimuksessaan tiettyä tapausta ja tietyn valtion journalisteja, valtiot valvovat kansalaisiaan ainakin jollain tasolla maailmassa.

Journalistin ja lähteen välisen turvallisen kanssakäymisen puolesta puhuu myös teknologiatoimittaja ja tietoturvainsinööri Micah Lee. Hän toteaa haastattelussaan (Lee & Heinrichs, 2019), että journalistin täytyy puhelimen lisäksi käyttää työssään tietokonetta ja internetiä, joihin molempiin jää väistämättä jälkiä käyttäjän toiminnasta. Tämän vuoksi on tärkeää, että journalisti ymmärtäisi oman roolinsa siinä tapauksessa, jos viestitään arkaluontoisia tietoja paljastavan pilliinviheltäjän (engl. whistleblower) kanssa. Huomionarvoisaa on myös Leen toteamus siitä, että lähdesuojan ja pilliin viheltäjien suojaaminen koskettaa niin lehdistönvapautta kuin yleistä totuuden kertomista yhteiskunnassa. Lee nostaakin lähdesuojauksen yhdeksi tärkeimmäksi journalistin haasteeksi. Hänen mukaansa (yhdysvaltalais-)uutisorganisaatiot saavat digitaalisen turvallisuuden koulutusta ja ymmärtävät näin salatun viestinnän merkityksen – jopa enemmän kuin lähteet. Erityisesti valtiollisia ja kansallisen turvallisuuden parissa työskentelevät tutkivat toimittajat ovat oman kyberturvallisuustietämyksensä varassa (Lee & Heinrichs, 2019).

2.3 Journalismin tietoturvauhkat

Journalistit ovat hallussaan pitämiensä tietojensa sekä julkisen vaikutusvaltansa vuoksi arvokkaita tietomurron sekä häirinnän kohteita. Uhkat ja riskit liittyvät toimittajien vastuuseen pitää arkaluontoinen tieto salassa, mutta myös toimittajiin henkilökohtaisesti kohdistuvaan häirintään, kuten maalittamiseen sosiaalisessa mediassa. Aiemmasta tutkimuksesta voidaan nähdä, että suhtautuminen tietoturvan vaihtelee toimituksissa ja toimittajat voivat olla osaltaan jopa henkilökohtaisesti vastuussa tietoturvaratkaisuistaan, vaikka työskentelisivätkin työnantajan leivissä.

Aluksi on tärkeä avata keskeisiä termejä, joita ovat tietoturvauhka ja kyberuhka. Ne linkittyvät toisiinsa tietoon liittyvän uhkan kautta. Termillä kyberuhka voidaan tarkoittaa Saara Janssonin ja Tarja Sihvosen (2018) mukaan kaikkea ”-- pahantahtoista tarkoitusta vahingoittaa tai tuhota tietoverkkoa, tietojärjestelmää tai päätelaitetta”. Suomen valtion kyberuhkamalli jakaa kyberuhat viiteen kategoriaan. Näitä ovat kyberaktivismi, kyberrikollisuus, kybervakoilu, kyberterrorismi- ja operaatiot sekä kyberoperaatio, jolla painostetaan konfliktiin tai sotaan. Laajemmassa mittakaavassa kyberuhka voi tarkoittaa rikollisuuden lisäksi vakoilua ja sodankäyntiä. Informaatiosotaa- tai vaikuttamista ei kyberturvallisuuden tutkimuksessa välttämättä suoraan määritetä kyberuhaksi, sillä ne eivät tutkimuksen mukaan välttämättä suoranaisesti häiritse toimintaympäristön teknologista puolta. Informaatiosodankäynti- ja vaikuttaminen voidaan silti nähdä uhkaavina, sillä niillä pyritään vaikuttamaan ihmisten tai valtiotahojen päätöksentekoon suorasti tai

epäsuorasti. (Jansson & Sihvonen, 2018). Tietoturvauhka taas tarkoittaa laajemmassa käsityksessä tietoturvaan kohdistuvaa ja sen vaarantavaa haitallista tapahtumaa tai kehityskulkua (Turvallisuuskomitea, 2018, s. 25)

Journalismissa tieturvauhkat ja kyberuhkat liittyvät olennaisesti toimittajien tekemään arkaluontoiseen työhön, joka käytännössä vaatisi tiukkojakin salaustoimenpiteitä ja menetelmiä. Silti näin ei käytännössä aina ole – aiemman tutkimuksen perusteella uhkiin varautuminen vaihtelee hyvinkin paljon. Toimitusorganisaation sekava ja osin kaoottinenkin lähestymis- ja suhtautumistapa tietoturvaan altistaa digitaaliseen työympäristöön siirtyneet journalistit ja toimitukset vakavillekin tietohyökkäyksille (Watkins & Roesner, 2017). Journalismin tekijät ovat erityisen arvokkaita kohteita kyberhyökkääjien silmissä, koska he pitävät usein hallussaan arkaluontoista tietoa. Journalistien kohtaama tietotekninen vaikuttaminen on yksi journalismiin kytkeytyvä ulkoisen vaikuttamisen keino. Tämä vaikuttaminen kohdistuu Ilmari Hiltusen (2020) mukaan toimittajien työvälineisiin ja tietoverkkoihin. Erilaisia vaikuttamiskeinoja ovat verkkovakoilu, verkkohyökkäykset ja murtautumisyritykset esimerkiksi sähköposteihin, sosiaalisen median profiileihin ja toimitusten järjestelmiin. Vaikuttajan motiivina voi olla arkaluontoisen tiedon hankkimista esimerkiksi lähteestä tai journalistin yksityiselämästä. Tavoitteena voi olla myös toimituksen suora vakoilu (Hiltunen, 2020).

Toimitustyö on monin tavoin autonomista ja näin vaikuttaa olevan myös tietoturvan kanssa – eikä tämä ole hyvä asia. Toimituksilla ei välttämättä ole yhtä strategiaa tai puolustautumistapaa esimerkiksi tietojenkalastelua vastaan, vaan tietosuoja jätetään yksittäisten toimittajien ja jopa lähteiden harteille. Tämä juontaa juurensa siitä, että uutistoimituksissa on nimenomaan totuttu kunnioittamaan journalistista autonomiaa. Tämä näkyy valitettavasti tietoturvakäytännöissä: toimittajat valitsevat itse itselleen sopivimman tavan tietoturva-asioissa eikä lopputulos ole aina lähelläkään hyvää (Watkins & Roesner, 2017). Tästä koituu tietoturvallinen tyhjiö toimituksissa: autonomian ja puutteellisen strategian vuoksi ilmiö aiheuttaa tietoturvalle ongelmia.

Tietoturvan itsensä takia on tarkasteltava myös niitä uhkia ja riskejä, jotka eivät ole tehty valtiotahojen tai rikollisten toimesta. Näitä ovat esimerkiksi trollaus, häirintä ja maalitus sekä kiusaaminen. Silvio Waisbordin (2020) vastikään tehty tutkimus paneutuu journalistien kokemaan verkkohyökkäyksiin (engl. online attacks). Yleisimpiä häirinnän ja trollauksen muotoja ovat haukkuminen, verbaalinen aggressio ja osin myös ideologinen kielenkäyttö. Kaikki journalistit eivät kuitenkaan ole yhtä alttiita verkkohyökkäyksille: tutkimus toteaa, että kohteen huomioarvoa lisäävät esimerkiksi sosiaalisen identiteetin, kuten sukupuolen, etnisyyden,

seksuaalisuuden ja uskonnon julkinen näkyminen (Waisbord, 2020). Tutkimuksen anti sopii sinällään oman tutkimukseni verkkohyökkäyksen ja häirinnän teemaan, vaikka se onkin tehty yhdysvaltalaisesta näkökulmasta ja vieläpä niin, että tutkimuksen keskiössä on antijournalistinen häirintä yhteiskunnallisella tasolla. Tällä viitataan erityisesti presidentti Donald Trumpin valtakaudella yleistyneeseen median ja toimittajien häirintään, demonisointiin ja maalittamiseen.

Uhkia vastaan voi, ja kannattaa toki varautua. Käytännön journalistisista tietoturvametodeista kirjoittanut tanskalainen toimittaja ja digitaalisen turvallisuuden opettaja Freja Wedenborg (2015) kannustaa toimittajan omaan aktiivisuuteen tietoturvan säilyttämisessä. Keinoja on jo aiemmin mainitusta teknologisen osaamisen parantamisesta asennemaailman tarkasteluun – toimittajan on tärkeää suhtautua tietoturvaan arkisena, pysyvänä ilmiönä, jota tilanteen vaatiessa ruuvataan tiukemmalle (Wedenborg, 2015).

Yhteenvetona voidaan todeta, että journalismin ja tietoturvan suhde on laaja ja monimutkainen: sitä voidaan tutkia sekä välineellisen että kulttuurisen määrittelyn kautta (Di Salvo, 2022) eikä tämäkään linja ole kiveen hakattu. Tietoturvaa journalismissa leimaa toimittajien, toimitusten sekä hallintoportaiden ymmärryksen puute siitä, mitä tietoturvalla oikeastaan tarkoitetaan ja miten sitä toteutetaan käytännössä. Yleinen ongelma on, että jos tietoturvaa ei koeta tärkeäksi oman työnkuvan kannalta, siihen ei tarvitse panostaa. Samalla kun yksittäiset toimittajat vastuutetaan hoitamaan omia tietoturvaratkaisujaan, on olemassa joukko tietoturvasta kiinnostuneita toimittajia, jotka kenties yrittävät muuttaa toimituksen käytäntöjä paremmiksi siinä statuksen puuttuessa kuitenkaan onnistumatta. Huoli lähdesuojan turvaamisesta on ollut esillä tutkimuskentällä jo pitkään eikä sen haavoittuvuus ole kadonnut, päinvastoin – maailman edetessä kohti valvotumpaa globaalia yhteisöä kohti ongelmat lähdesuojan turvaamisessa tulevat mitä todennäköisimmin vain jatkumaan varsinkaan jos journalismikenttä ei ota tietoturvariskejä vakavasti koko organisaatiorakenteen osalta. Välineellisen kulttuurin kautta on mahdollista tutkia esimerkiksi sangen uutta ilmiötä, varjo-IT:tä, jonka olemuksesta journalismissa olisi hyvä saada lisää tietoa jatkotutkimusten avulla.

3 AINEISTO JA MENETELMÄT

Tässä luvussa esittelen ja käsittelen käyttämäni aineistonhankintamenetelmät ja analyysimenetelmän. Ensin selostan haastateltavien valintaprosessin ja avaan käyttämäni haastattelumetodin, puolistrukturoidun teemahaastattelun. Tämän jälkeen puran auki haastattelujen toteutuksen. Lopuksi selostan käyttämäni analyysimenetelmän, temaattisen sisällönanalyysin vaiheineen.

3.1 Haastateltavien valinta

Tutkimukseen valitsin suomalaisessa mediatalossa kokoaikaisessa työsuhteessa tai siihen verrattavassa työsuhteessa olevia toimittajia. Tavoitteenani oli, että jokainen haastateltava olisi eri mediatalosta. Näin tutkimukseni tuottaisi mahdollisimman kattavan kuvan suomalaisen mediakentän tietoturvakokemuksista eikä keskittyisi esimerkiksi vain yhden mediatalon työntekijöiden kokemuksiin.

Jo tutkimuksen varhaisessa vaiheessa minulla oli mielessäni viisi potentiaalista haastateltavaa, jotka sopisivat työnkuvansa ja työkokemuksensa perusteella tutkimukseen. Tiesin heidän erikoisalansa julkaistujen juttujen ja sosiaalisen median toiminnan perusteella. Potentiaalisten haastateltavien lähestyminen oli suoraviivaista: lähetin sähköpostitse esittelyn tutkimuksestani ja kysyin halukkuutta osallistua siihen.

Suorien haastattelupyyntöjen lisäksi käytin niin sanottua *lumipallo-otantaa*, jossa avainhenkilö tai -henkilöt johdattavat tutkijan tiedonantajasta seuraavaan (Tuomi & Sarajärvi, 2018, s. 76). Avainhenkilöitä minulla oli yhteensä kolme. Heidän vinkkiensä avuilla sain haastattelukutsun lähetettyä lopulta yhteensä viidelletoista toimittajalle. Koko kysyttyjen joukosta yhteensä neljä suostui aikatauluni puitteissa haastatteluun.

Kaiken kaikkiaan kaksi kieltäytyi haastattelusta ja yhdeksän ei vastannut sähköpostiin.

Haastateltavien joukko edusti tutkimusongelman kannalta oleellista ja moninaista joukkoa, ja he kaikki työskentelivät eri työnantajilla. Työhistorian lisäksi työtehtävät vaihtelivat hieman toimittajasta toiseen, joka toi vaihtelevuutta haastatteluihin.

Täsmennyksenä haastateltavien valintaan mainittakoon, että en tuntenut ketään haastateltavaa ennakolta, edes kollegiaalisesti. Kaikki tutkimukseen mukaan lähteneet toimittajat olivat siis tutkijalle ennestään tuntemattomia.

3.2 Puolistrukturoitu teemahaastattelu

Haastattelut tein puolistrukturoitua teemahaastattelumenetelmää käyttäen. Teemahaastattelu on sangen vapaamuotoinen: se etenee ennalta valittujen, suurempien teemojen mukaisesti. Etukäteen valitut teemat luodaan tutkimuksen viitekehykseen, joka muodostuu siitä, mitä tutkittavasta ilmiöstä tiedetään (Tuomi & Sarajärvi 2018, s. 68).

Teemahaastattelu sopii tutkielmaani, koska siinä korostetaan ihmisen – tässä tapauksessa haastateltavan – omakohtaisia tulkintoja sekä merkityksiä. Strukturoidun haastattelun sijaan näen parempana, että haastattelutilanteessa voi reagoida saman aihepiirin sisältä tulevaan informaatioon esimerkiksi jatkokysymyksillä. Lisäksi haastateltava ei ole sidottu vastausvaihtoehtoihin tai tiukkoihin raameihin, vaan voi muotoilla itse näköisensä vastauksen – ja ehkä jopa keskustella laajemmin aiheesta, kun sitä ei ole rajattu tiukasti.

Teemahaastattelu koostui kolmesta pääteemasta, *toimittajien yleiset kokemukset tietoturvasta toimitustyössä*, *kyberturvallisuusuhkien ymmärtäminen ja riskitekijät toimitustyössä* ja *teknologiaan keskittyvä osuus,* jossa käsiteltiin haastateltavien toimitustyössään käyttämiä teknisiä työvälineitä ja haastateltavien suhtautumista niiden tietoturvaan. Näiden teemojen lisäksi jokaisessa haastattelussa käytiin läpi haastateltavien henkilötiedot sekä työhistoria ja opiskelutausta, jotka toimivat osaltaan myös haastattelun tutustumisprosessia. Anonymiteetin suojelemiseksi koin kuitenkin lopulta tärkeänä, että mitään näistä tiedoista ei käytetä valmiissa raportissa.

Haastattelutilanne antaa vapauksia sekä haasteltavalle että haastattelijalle. Hirsjärvi ja Hurme (2001) katsovat, että haastattelutilanteen eduiksi voi laskea muun muassa

haastateltavan näkemisen subjektina – hänellä on tutkimustilanteessa mahdollisuus ilmaista itseään koskevia asioita mahdollisimman vapaasti. Lisäksi tutkijalla on mahdollisuus edetä ”vähän kartoitetulla alueella” syvemmälle haastattelussa, jos vastausten suuntia on voinut olla vaikea tietää ennalta. Haastattelu antaa lisäksi mahdollisuuden jatkaa tiedonhankintaa syventävillä kysymyksillä (Hirsjärvi & Hurme 2001, s. 35). Puolistrukturoitu haastattelumuoto antaa vapauden lisäksi vastuuta. Ei ole yhdentekevää, millaiseksi teemat muotoilee tai kuinka niissä pysyy – tai ei pysy – haastattelutilanteessa. Tuomen ja Sarajärven (2018) mukaan on makuasia, kysyykö kaikilta haastateltavilta samat suunnitellut kysymykset, esitetäänkö ne samassa kronologisessa järjestyksessä haastattelutilanteessa, tai että pitääkö kysymysten sanamuotojen olla täysin samat jokaisessa haastattelutilanteessa. Haastattelun eduiksi voidaan katsoa myös sen sitovuus. Kun haastatteluluvasta sovitaan etukäteen, haastateltavat harvoin peruvat osallistumistaan. Näin kävi tässäkin tutkimuksessa. Kaikki haastateltavat pitäytyivät osallistumisessaan ja sovitussa aikataulussa (Tuomi & Sarajärvi, 2018, s. 67–68).

3.3 Haastattelujen toteutus

Haastattelut neljän haastateltavan kanssa sovittiin vuoden 2022 alkuun, tammikuuksi heti joululomakauden loputtua. Jokaisen haastateltavan kanssa käytiin sähköpostikeskustelu ajankohdan varmistuksesta sellaiseksi, joka takaisi tutkimushaastattelulle häiriöttömän ajankohdan. Koska haastattelut tehtiin koronapandemiasta johtuen etänä, tämä tarkoitti haastateltavan sijoittumista sellaiseen tilaan, jossa häiriötekijöitä, kuten kollegoita tai perheenjäseniä, olisi mahdollisimman vähän. Haastattelujen sopimisen jälkeen lähetin haastateltaville tutkimukseen liittyvät tietosuojailmoituksen ja tutkimussopimuksen.

Teemahaastattelun runkoa, teemoja tai haastattelijan apukysymyksiä ei käyty haastateltavien kanssa etukäteen läpi. Tämä oli tietoinen valinta, joka takasi haastateltavan tietotason aiheesta olevan sillä tasolla kuin se realistisesti olisi ilman etukäteisperehtymistä. Haastateltavia ei kuitenkaan erikseen kielletty perehtymästä aiheeseen, mutta heitä ei myöskään kannustettu siihen. Tutkimuksen analysointivaiheen kannalta oli oleellista, että haastateltavat olivat haastattelutilanteessa niin sanotusti kylmiltään – halusin haastateltavien kokemukset ja tuntemukset kaunistelemattomina.

Haastattelut järjestettiin etäyhteydellä koronapandemian ja välimatkojen takia. Etähaastattelut tehtiin Zoom-sovelluksella, jolla haastattelut myös tallennettiin.

Etähaastatteluissa ei ollut ongelmia – kaikki osapuolet olivat jo tottuneet etävälineisiin työssään ja arjessaan.

Neljän haastattelun yhteiskestoksi muodostui 188 minuuttia. Pisin haastattelu oli kokonaiskestoltaan 57 minuuttia. Lyhyin keskustelu kesti kaikkiaan 38 minuuttia. Yksi haastattelu kesti keskimäärin 47 minuuttia.

Koska haastattelut tehtiin täysin etäyhteydellä, nauhoitus oli päällä jo heti keskustelun alussa. Tämän vuoksi ”small talk” jokaisen haastattelun alussa – tutustuminen, kuulumisten kysely, tutkimuksesta keskustelu –vievät haastattelujen kestoa alaspäin. Varsinaisen asiasisältöisen haastattelun kestoksi jää siis keskimäärin 42 minuuttia. Tämä tarkoittaa noin viittä minuuttia kevyempää keskustelua ennen varsinaisen asiakeskustelun aloitusta per haastattelu.

Haastatteluaineisto litteroitiin Wordin litterointiominaisuutta ja yksityiskohtaisempaa tarkistusta käyttäen. Käytännössä jokainen haastattelunauhoitus vietiin Wordin litteroinnin kautta tekstidokumenttiin, joka käytiin läpi suorat virheet korjaten kertaalleen nauhoitus kuunneltuna. Litteroitua haastattelumateriaalia tuli yhteensä 130 A4 -sivua.

3.4 Anonyymius ja sen merkitys haastateltavalle

Tässä tutkimuksessa kukaan haastateltavista ei esiinny omalla tai edes keksityllä nimellä. Sitaateissa tai tulosten selvityksessä ei ole kirjattuna mitään sellaista, mistä yksittäisen haastateltavan voisi tunnistaa. Tämä on tietoinen valinta, jonka avulla halusin suojella haastateltavien henkilöllisyyttä. Perimmäinen tarkoitus on suojella tutkimukseen lähteneiden henkilöllisyyttä ja estää ongelmat esimerkiksi työsuhteissa. Anonymiteetti oli selvää jo heti alusta lähtien: esitin jo tutkimuskutsussa, että työ käsittelisi kokemuksia nimettömänä, ilman tunnistettavia tekijöitä. Tämä oli tulkintani mukaan haastateltaville tärkeä keskustelua helpottava menetelmä, sillä näin he pystyivät kertomaan esimerkiksi mahdollisista epäkohdista ja ongelmista avoimemmin kuin nimellään esiintyen.

Haastateltavien anonymiteettia suojellakseni tuhosin kaikki haastatteluäänitteiden tiedostot heti onnistuneiden litterointien jälkeen. Litterointitiedostoihin haastateltavat saivat tunnistenimet *”Haastateltava + numero”*.

3.5 Analyysi

Analyysimenetelmänä käytin tässä tutkimuksessa laadullista sisällönanalyysia, josta tarkemmin teemoittelua, ts. temaattista sisällönanalyysia. Sitä käyttämällä aineistosta paikannetaan aiheet, eli teemat, jotka ovat olennaisia tutkimusongelmaa vasten katsottaessa. (Juhila, K. Laadullisen tutkimuksen verkkokäsikirja).

Temaattinen analyysi voidaan tehdä joko aineisto- tai teorialähtöisesti. Omassa tutkimuksessani teemat muodostuivat aineistolähtöisesti, eli havainnoin aineistosta nostamiani huomioita, joista muodostin Tuomen ja Sarajärven (2018) temaattisen analyysin mallin mukaisia teemakokonaisuuksia. Sisällönanalyysin ja temaattisen analyysin esiintyminen samassa asiayhteydessä voi olla hämmentävää (Tuomi ja Sarajärvi, 2018, s.110–111), sillä ne vaikuttavat peruspiirteiltään hyvin samankaltaisilta. Eroja näistä kahdesta löytyy kuitenkin aineiston käsittelystä. Temaattisessa analyysissa aineisto hajotetaan lopulta kartaksi, esimerkiksi käsitekartaksi, siinä missä sisällönanalyysissa aineisto pirstotaan pelkistetyiksi ilmaisuiksi, joista analyysin käsitteet muodostetaan. Kahden toisiaan lähellä olevan analyysin toimintatavat ovat kuitenkin Tuomen ja Sarajärven (2018) tulkinnan mukaan vain pinnallisia ja toimintamallit aineistoon tutustumisesta aina kiinnostavien asioiden pelkistämiseen ovat täysin verrattavissa toisiinsa (Tuomi & Sarajärvi, 2018, s. 111).

Koin temaattisen analyysin sopivan parhaiten tutkimukseeni laadullisen sisällönanalyysin menetelmistä, koska se mahdollistaa Tuomen ja Sarajärven (2018) mukaan laadullisen aineiston pilkkomisen ja ryhmittelyn aihepiirien mukaisesti. Menetelmä painottaa sitä, mitä kustakin teemasta on sanottu eikä sanottujen asioiden lukumäärillä ole merkitystä toisin kuin sisällönanalyysin tekemistä luokittelun keinoin, jossa aineistosta määritellään luokkia ja niiden esiintyvyys lasketaan (Tuomi & Sarajärvi, 2018, s. 105). Temaattinen analyysi mahdollisti omassa tutkimuksessani yksittäisten haastateltavien huomioiden, esimerkiksi kokemusten tai pohdinnan, nostamisen esille ja se oli näin tehokas keino vastata tutkimuskysymyksiin, joilla haettiin kokemus- ja käsitysperäistä tietoa. Kuten jo todettu, analyysini perustuu aineistoon, eli sitä kutsutaan aineistolähtöiseksi sisällönanalyysiksi, jossa analyysiluokat, kuten tässä tapauksessa teemat, luodaan (tai ”nostetaan”) aineiston, ei teorioiden, kautta. Tuomi ja Sarajärvi (2018) kuitenkin muistuttavat tutkijan roolista analyysivaiheessa: aineistosta ei itsekseen ”nouse” mitään teemaa, vaan teeman luominen on aina tutkijan aktiivisen toiminnan tulos (Tuomi & Sarajärvi, 2018, s. 144).

Oma temaattinen analyysini aineiston parissa alkoi haastatteluihin paneutumisella, eli käytännössä lukemisella. Luin kaiken litteroidun haastattelumateriaalin, yhteensä 130 A4-sivua, kaksi kertaa etsien toistuvia teemoja ja usein esiintyviä piirteitä, mutta myös eroavaisuuksia, jotka voisivat tuoda uutta tietoa tai näkökulmaa tutkimukseeni.

Ensimmäisessä analyysivaiheessa nostin esille tutkimuskysymyksiin vastaavia sisältöjä värikoodaamalla haastateltavien sitaatteja Wordissa. Lukemis- ja koodauskertojen aikana tein lisäksi muistiinpanoja ja havaintoja haastateltavien vastauksista ja kommenteista koskien tutkimukseni aihetta ja tutkimusongelmaa. Tämän jälkeen etenin yksittäisten sitaattien värikoodaukseen, jonka tein jokaisessa neljässä haastateltavan dokumentissa. Jätin selvästi tutkimukseni aiheen ulkopuolisen keskustelun ja kommentoinnin koodaamatta ja täten huomiotta.

Temaattinen analyysi jatkui tämän jälkeen värikoodatun sitaattimateriaalin siirtämisellä Excelin taulukkorunkoihin. Teemat, jotka rajasin aineistosta ovat:

- Toimittajan oma käsitys toimitustyön tietoturvauhista
- Pohdintaa toimittajan tietoturvaosaamisesta
- Toimittajan esille nostamat koulutus- ja osaamistarpeet
- Mistä toimittaja hakee apua tietoturvahaasteita kohdatessaan
- Toimittajan vinkit journalistisen tietoturvan parantamiseen
- Toimittajan näkemys työnantajan roolista tietoturvallisessa työskentelyssä

Excelin dokumentin jaoin kuuteen alasivuun, joista jokainen vastasi yhtä temaattisen analyysin pääteemaa. Siirsin litterointidokumenteista kaikki tutkimuksen kannalta oleelliset sitaatit Excelin teemasivuille niin, että vielä tässä vaiheessa jokaisella haastateltavalla oli oma sarakkeensa. Yksittäisten teemojen käsittelyä helpotin jaottelemalla pääteemoja alateemoiksi. Esimerkiksi ensimmäisen pääteeman ”Käsitys toimitustyön tietoturvauhista” alateemoiksi nostin muun muassa ”Toimittajan riskipaikat”, ”Kyberuhan ymmärtäminen” ja ”Lähdesuojan merkitys”. Tällä tavalla aineistoa jäsentelemällä loin teemaluokan jokaiselle tutkimustani koskevalle aiheelle, josta haastateltavat aineistossa puhuivat.

Olin jo litterointivaiheessa muuttanut haastateltavien nimitunnisteet muotoon Haastateltava 1, Haastateltava 2,… ja sama koodaustyyli jatkui analyysin loppuvaiheessa jatkuen aina tulosten esittämiseen. Analyysivaiheessa haastattelumateriaalia eli sitaatteja ei vielä siivottu puhekielisyydestä tai äännähdyksistä, vaan kommentit kopioitiin suorasta litteroinnista. Sitaattien kevyt

editointi, joka suurelta osin tarkoitti Wordin litterointiohjelman asettamien välimerkkien poistamista, tapahtui raportointivaiheen lopuksi.

Vaihtoehtoinen menetelmä koko haastattelupolulle olisi voinut olla esimerkiksi kysely, jota myös pohdin vakavasti tutkimussuunnitelmassa. Kyselyllä olisin voinut tavoittaa laajemman joukon toimittajia, joka olisi tarkoittanut laajempaa kokonaiskuvaa suomalaisesta mediakentästä. Toisaalta taas koin kyselylomakkeen raskaaksi ja kankeaksi, jopa liian helposti sivuutettavaksi – se kun on jopa liiankin helppo poistaa sähköpostista työpäivän kiireessä. Suurin kysymykseni oli kuitenkin se, millä keinolla tavoittaisin toimittajia kyselyä varten. Toimitusyhdistyksistä, työnantajilta? En myöskään usko, että olisin saanut syvällisiä vastauksia kyselytutkimuksesta, vaikka olisinkin sisällyttänyt siihen vapaasti täytettäviä lomakkeita. Valitsemani haastattelumetodin vahvuus on nimenomaan siinä, että Tuomen ja Sarajärven (2018) mukaan se soveltuu erityisesti ihmisten tulkintojen ja asioilleen antamien merkitysten etsimiseen. Lisäksi puolistrukturoidun teemahaastattelun avoimuus antaa mahdollisuuden intuitiivisten ja kokemusperäisten havaintojen selvittämiseen (Tuomi & Sarajärvi, 2018, s. 87–88).

4 TULOKSET

Tässä luvussa esittelen aineistosta nousseita teemoja, jotka vastaavat kahteen tutkimuskysymykseen, *miten toimittajat kokevat tietoturvallisuuden osana työtään* ja *millaisia tietoturvauhkia toimittajat mahdollisesti kokevat työssään*.

Analyysissa käyttämieni koodausluokkien ja teemoittelun kautta muodostin aineistosta kolme suurempaa teemakokonaisuutta, *tietoturvan teoreettiset uhat, osaaminen ja yhteiset pelisäännöt ja työnantajan rooli.* Päädyin aineiston kuuden teemaluokan tiivistämiseen kolmeen tutkielman selkeyden vuoksi. Teemat päätyivät yhteen samankaltaisen, laajemman aihepiirin kautta: esimerkiksi osaamisen ja koulutustarpeiden teemojen yhdistyivät teemakokonaisuuden *osaaminen ja yhteiset pelisäännöt* alle.

Ensimmäisessä alaluvussa käsittelen aineistosta nostamiani tietoturvaan ja tietoturvariskeihin ja -uhkiin liittyviä kokemuksia ja mietteitä. Toisessa alaluvussa suunvuoron saavat toimittajien omat käsitykset omista tietoturvataidoistaan sekä koulutus- ja osaamistarpeet. Lisäksi esittelen haastatteluissa esiin tulleita kriittisiä näkemyksiä. Kolmannessa ja viimeisessä osassa käsittelen sitä, miten haastateltavat kokevat työantajan roolin tietoturva-asioissa. Työnantaja on kriittisessä asemassa työn tietoturvan mahdollistajana ja haastateltavat toimittajat kertovat oman näkökulmansa työnantajien toimista anonymiteetin turvin.

4.1 Tietoturvan teoreettiset uhat

Tietoturva koettiin kaikissa haastatteluissa laajaksi ja osin abstraktiksi aiheeksi. Aineiston mukaan tietoturvallinen työ tarkoitti esimerkiksi työn tekemistä niin, ettei ei-toivottua tietoa tai salaisuuksia paljastu ulkopuolisille tai väärille tahoille.

Eräs haastateltava määritteli tietoturvaa työssään ytimekkäällä kiteytyksellä:

> Jos meillä on tietokoneella jotain arkaluontoisia asioita, niin kukaan ei niitä pääse nappaamaan, näin lyhykäisyydessään. (Haastateltava 1)

Arkaluontoiset asiat tarkoittavat aineiston perusteella digitaalisen materiaalin lisäksi muun muassa viestinvaihtoa, muistiinpanoja ja esimerkiksi lähteiden nimiä. Myös toimituksen työpöydillä olevat tulosteet, asiakirjat ja muistiinpanot koettiin tietoturvan käsitteen alaisiksi.

Tietoturvaan paneutuva puhe keskittyy suurelta osin uhkakuviin ja riskeihin ja haastateltavat määrittelivätkin näitä huomattavasti laajemmin kuin abstraktimpaa kattotermiä.

Kyber- ja tietoturvauhka terminä sai haastateltavat pohtimaan yhteiskunnallista vaikuttamista. Termit veivät ajatukset valtiotason uhkakuvaan ja yhteiskuntaan liittyvään kriisiin. Aineiston mukaan kyberuhka on lähtöisin valtion toiminnasta ja kohdistuu toisen valtion infrastruktuuriin tai suuriin yrityksiin. Eräs haastateltavista pohti yhteiskunnallista uhkaa vielä pidemmälle, valtiotasojen pimeämmälle ja salaiselle puolelle: hänen mukaansa voidaan olettaa, että valtioilla on kiinnostusta vakoilla toimittajia.

Mediaan kohdistuva tietoturvauhka taas nähtiin aineistossa ensisijaisesti journalistisen työnteon konkreettisena haittaamisena. Esimerkkejä tästä ovat verkkoyhteyksien katkaisu tai palvelinestohyökkäykset, joiden avulla median toiminta pysähtyisi tai hankaloituisi merkittävästi.

Lähdesuojalla on aineistossa merkittävä rooli. Kaikki haastateltavat korostivat lähdesuojan turvaamisen tärkeyttä. Yhdistävä teema ja aineistossa toistuva huolenaihe on lähteen henkilöllisyyden vaarantuminen ja pelko siitä, että toimittajan lähteelle lupaama lähdesuoja murtuisi tai murrettaisiin.

> --aika useinhan siinä kun mietitään, että pysyykö tieto suojassa niin kysymys ei ole niinkään siitä, että pysyykö toimittajan tiedot suojassa vaan siitä, että pystytäänkö lähdesuoja takaamaan niille henkilöille, jotka luottavat toimittajaan ja ovat valmiita kertomaan luottamuksellisia asioita. (Haastateltava 3)

Pelkästään toimittajalta lähteelle -suunta lähdesuojan vastuukysymyksessä ei tyydyttänyt kaikkia tutkimukseen osallistuneita. Yksi esimerkki on tapaus, jossa lähde lähestyy toimittajaa turvatonta kanavaa pitkin. Alla oleva lähestymistapa aiheuttaa haastateltavan mukaan päänvaivaa, jos lähde itse ei ymmärrä tietoturvallisen viestinnän perään:

> Välillä on ollut sellaisia tilanteita, että henkilö saattaa laittaa viestin, että hei, minulla olisi tällainen tosi kuumottava epäkohta ja olen halunnut tästä puhua ja voisimmeko puhua luottamuksellisesti, entä lähdesuoja. Ja sit näen siitä viestistä, että hän on lähettänyt sen työnantajan sähköpostista. Niin sitten on tavallaan sellaisissa tilanteissa hankala, että sä et enää toimittajana pysty tavallaan auttamaan sitä. (Haastateltava 3)

Entä sitten yksittäiseen toimittajaan kohdistuva tietoturvauhka? Tämä nähtiin toimittajaan tai hänen lähipiiriinsä kohdennettuna tekona, joka toteutetaan digitaalisissa kanavissa, kuten sosiaalisessa mediassa. Maalittamiskampanjat tai somehäirintä toistuvatkin aineistossa useasti eri kommenteissa. Yhteistä niille on se, että joku ulkopuolinen taho saisi jotain kautta käsiinsä toimittajan työhön tai henkilökohtaisuuksiin liittyvää tietoa.

> Sellanen kauhukuva mulla on, että joku pääsisi niinku käsiksi mun viestiliikenteeseen, julkaisisi sen jossain verkossa tai kaivaa mun kaikki jotkut pilvessä olevat dokumentit auki. Tai siis niinku tää vastaamon [Psykoterapiakeskus Vastaamo] keissi, niin kyllähän tällaisilla toimittajaa voitaisiin kiristää ja lamauttaa, saada ihminen toimintakyvyttömäksi henkisesti. (Haastateltava 3)

Toimittajaan kohdistettu henkilökohtainen, tietoturvaan liittyvä teko tuntui erään haastateltavan mukaan hyvin epämiellyttävältä. Hän myös pohti omia valmiuksiaan kyberuhan torjumiseksi melko pessimistisin sanoin:

> -- ei ole mukava asia, että joku luultavasti pystyy seuraamaan työtäni, joku josta en tiedä kuka se on. Se, miten näitä tietoja käsitellään, niin ole ihan varma onko mulla riittäviä valmiuksia tai työvälineitä siihen. (Haastateltava 2)

Tietoturvauhkia- ja riskejä löytyi aineistosta työn lisäksi vapaa-ajan aktiviteeteista ja ihmisyydestä itsestään. Inhimillisyys ja arjessa tehdyt virheet tulivat esiin erään haastateltavan pohdinnassa, jossa huolimattomuus on riski lähdesuojalle.

Työelämä ja vapaa-aika peilautuvat aineistossa osin ristiin. Eräs haastateltavista lokeroikin toimitustyön tietoturvahaasteet samaan kategoriaan vapaa-ajan tietoturvahaasteiden kanssa. Hänen mukaansa olisi ymmärrettävä, että työn tietoturvauhat ovat samoja digitaalisen arjen uhkia, joita kuka tahansa verkkoa käyttävä henkilö voi päivittäin kohdata. Esimerkeiksi haastateltava nosti arjesta tutut sähköpostihuijaukset, tietojenkalasteluyritykset ja tietokoneiden haittaohjelmat. Samalla hän tosin pohti, että toimittajia vastaan kohdennetut tietomurtoyritykset ovat varmaankin kovin harvinaisia.

Työvälineiden ja omien laitteiden ristikäyttö on haastateltavien mukaan ongelmallista, vaikka sitä tapahtuu aineiston perusteella runsaasti. Aineiston perusteella haastateltavat käyttävät esimerkiksi henkilökohtaista puhelinta ainakin joissain määrin työasioissa ilman, että asiasta olisi sovittu tarkemmin työantajan kanssa. Tämä

nähtiin tietoturvariskinä, joka johtuu kontrollin puutteesta: työantajan tarjoama suoja ei kata henkilökohtaisia laitteita missään määrin.

> En tiedä miten meidän työpuhelimet on suojattu, minkälaiset suojaukset niissä on, mutta epäilen, että jonkunlaiset ne on kun ne on tuolta firmalta annettuja. En tiedä huomaisko ne jossain tuolla ylempänä jos joku meidän puhelimiin yrittäisi päästä, mutta mun oma puhelin on mun oma puhelin. Se sitten on ihan täysin mun varassa. (Haastateltava 1)

Vapaa-ajan riskit eivät aina liity huijauksiin tai hakkerointiin – dataa kun on miltei jokaisesta netinkäyttäjästä saatavilla julkisesti, joskus paljonkin. Esimerkiksi paikannustietoa käyttävät sovellukset, kuten Sports Tracker-urheilusovellus, esiintyivät aineistossa varteenotettavina uhkatekijöinä. Näissä sovelluksissa riski on erään haastateltavan mukaan siinä, että niiden tallentamaa ja usein verkossa julkaistua paikannustietodataa käyttämällä voidaan esimerkiksi seurata toimittajan liikkeitä ja tutkia, ketä hän on mahdollisesti tavannut. Seurannan toinen varjopuoli korostui pohdinnassa mahdollisten ulkomaille suuntautuvien työmatkojen yhteydessä. Seuranta nähtiin potentiaalisena riskinä turvallisuudelle, jos kohdemaana on esimerkiksi aktiivisesti kansalaistensa valvontaa toteuttava valtio.

Sosiaalinen media saa myös osansa tietoturvariskinä: aineistossa korostuu sosiaalisen median, erityisesti Facebookin ja WhatsAppin riskit salauksen osalta erityisesti lähdesuojasta keskustellessa. Eräs haastateltavista pohti kolmannen osapuolen viestintäpalvelun turvallisuutta, jos viestit ovat palvelimella paikassa, jossa tietoturvakäytännöt ovat ”lepsut”. Yleisesti voidaan todeta, että aineiston perusteella yleisempien viestintäalustojen, kuten Facebookin ja WhatsAppin, puutteet ja riskit tiedostettiin ja ainakin osin suosittiin tietoturvallisempaa Signal-sovellusta.

Tehokkaiden salasanojen käyttö nousi esiin aineistossa. Niin sanotut ”huonot, yksinkertaiset salasanat” laitteilla ovat riski toimittajan työssä, kuten myös tietovuodoissa mukana olleet salasanat. Salaus, tai oikeastaan sen puute, viestiliikenteessä esiintyy toistuvana huolenaiheena aineistossa lähdesuojan riskeistä puhuttaessa. Huoli koski sekä toimittajan että vastaanottajan päätä.

4.2 Osaaminen ja yhteiset pelisäännöt

Haastateltavien käsitys heidän omasta tietoturvaosaamisestansa on moninainen. Aineistossa korostuu eräänlainen hämmennys siitä, että haastateltavat joutuvat arvioimaan omia taitojaan alueella, jolla he eivät ehkä koe olevansa vahvoilla. Toisaalta haastateltavat löytävät osaamisestaan positiivista kulmaa, mutta osaamisen teema aineisto kallistuu enemmän huolien havainnointiin ja pohdintaan.

Eräs haastateltava kiteytti heti haastattelun aluksi pohdintansa tietoturvaosaamisestaan ”havahtumisen paikaksi” – hän ei ollut juurikaan pohtinut tietoturvaa työssään ennen tutkimuskutsun saamista.

> Oonkohan mä liian sinisilmäinen ja tavallaan luottavainen, kun mä tavallaan tiedostan, että näistä [tietoturva-asioista] täytyisi pitää huolta, mutta jotenkin luotan siihen, että jos joku lähettää mulle sähköpostia niin se on automaattisesti niin ettei siihen kukaan tule väliin. Ehkä kun mun ajatukset on tätä tasoa niin se kertoo varmaan siitä että aika lapsenkengissä meillä tämä on eikä tähän niin hirveästi kiinnitetä huomiota. Jotenkin ajattelen, että se [tietoturva] on semmoinen itsestään selvä asia. (Haastateltava 1)

Toimitustyö nähtiin tietoturvan suhteen eräänlaiseksi keskiviivalla kulkemiseksi: työtä tehdään niillä välineillä, jotka on annettu, eikä lopputulos välttämättä riipu pelkästään taidoista.

> Käytännössä me tehdään kaikenlaisia kompromisseja tietoturvan kanssa. Jos olisi jotain sensitiivistä, niin meidän välineet ei ole kyllä siinä kunnossa, että ne olisi kovin helppoa ehkä tehdä mitään semmoista juttua, mikä vaatisi sen että pystyttäisiin blokkaamaan jotain tai ettei kukaan pääse tietoihin käsiksi. (Haastateltava 2)

Osaamisen puutteet huolettivat erityisesti tilanteissa, jotka tulevat yllättäen. Ongelmatilanteen hallitsemattomuus onkin yksi teema, joka toistuu toimittajien haastatteluissa. Tämä johtuu siitä, ettei toimintamalleja tietomurtoihin ja vastaaviin tapauksiin ole olemassa eikä niitä ole yksinkertaisesti harjoiteltu. Erä haastateltava kuvaakin omaa reaktiotaan kuvitteellisen tietomurron tilanteessa melkein humoristisin sanoin:

> -- kyllä mä niinku aika housut kintuissa olisin jos jotain tulisi. Yrittäisin soittaa IT-tuen numeroon, että hei nyt jotain tapahtui, että pelastakaa minut. (Haastateltava 1)

Aineistossa nousi esiin myös mielikuva työnkuvan vaikutuksesta tietoturvakäsitykseen: eräs haastateltavista oli tehnyt urallaan töitä rikosuutisoinnin parissa ja koki, että hänellä on tämän urakokemuksen myötä keskivertotoimittajaa parempi käsitys tietoturvallisesta työskentelystä. Kollegoiden erityisalalla on aineiston mukaan vaikutusta oletettuihin taitoihin.

> -- luulen, että tutkivilla journalisteilla on nämä vielä paremmin mietittynä, koska ne konkreettisesti tekee töitä semmoisten lähteiden kanssa, missä nämä pitää miettiä tarkkaan. Ehkä se yleisvaikutelma on, että he luultavasti miettii näitä asioita vähän aikaisemmassa vaiheessa. (Haastateltava 2)

Aineistossa esiintyy myös selvää huolta toimittajakollegoiden taidoista. Eräs haastateltavista toteaakin, että hänen mielestään ”moni kollega on joko aika pihalla tai välinpitämätön” tietoturva-asioissa. Sama huoli tulee esiin aineiston kautta. Esimerkkeinä tästä huolesta annetaan esimerkiksi kollegan tyylistä jättää arkaluontoiset työhön liittyvät paperit työpöydälle vartioimattomina.

Tietoturvan ja journalismin julkisuuskuva huolettaa aineiston perusteella haastateltavia. Aineistossa otettiin esiin esimerkkitapaus vuodelta 2017, jossa Puolustusvoimien Viestikoekeskuksesta kirjoittanut Helsingin Sanomien toimittaja yritti tuhota arkaluontoista, lähdesuojan alaista materiaalia sisältävän tietokoneensa vasaralla. Tämän johti tapahtumaketjuun, jonka seurauksena poliisi teki toimittajan kotiin kotietsinnän. Tapaus ja sen myötä nostetut oikeusjutut herättivät paljon keskustelua lähdesuojasta ja toimittajan roolista. Tapauksen julkisuuskuva ja yleisön reaktiot herättivät pohdintaa:

> -- en halua mitenkään väheksyä toimittajien osaamista tai heidän tietoturvataitojaan, mutta ehkä niinku ulospäin se näyttää siltä, että siellä ei välttämättä ollu nää hävittämiseen liittyvät menetelmät kovinkaan hyvin hallussa. Eli jollakin tavalla perustaitojen saaminen koko alalle voisi olla hyödyllistä. (Haastateltava 4)

Yhteinen aineistossa toistuva teema on oman perehtyneisyyden merkitys siihen, miten taidot koetaan. Eräs haastateltava sanoo suoraan, että hänen *pitäisi* olla paremmin perillä tietoturva-asioista ja käytettävistä sovelluksista, mutta kiireinen arki vie energian. Toinen haastateltava taas kertoo pitävänsä ”uuden oppimisesta varmuuden vuoksi”, mutta täsmentää olevansa epävarma esimerkiksi siitä, miten käytännössä arkaluontoinen liitetiedosto lähetettäisiin turvallisesti sähköisesti.

Aineisto tarjoaa näkökulma myös osaamisen tunnistamiseen ja suoranaisiin vinkkeihin haastavissa tilanteissa. Jokainen haastateltava löysi työarjestaan jotain, jota on tehnyt niin sanotusti oikein ja ajatuksella. Joku kertoo pitävänsä huolta, että kirjautuu palveluihin vain kaksivaiheista tunnistusta käyttäen ja miettii samalla virussuojausta sekä sitä, missä verkossa työkonettaan käyttää. Toinen täsmentää, että ei työ- tai vapaa-ajalla käytä mielellään julkisia verkkoja.

> Kun poistun tietokoneen äärestä, niin kyllä mä ainakin lukitsen aina sen. Mun mielestä nää on Ihan tämmöisiä perusjuttuja, että älkää nyt hyvät ihmiset jättäkö niitä koneita auki, että tänne [toimitukseen] voi joku tulla. (Haastateltava 1)

Työn ja vapaa-ajan eriyttäminen koettiin tärkeänä erityisesti teknologian osalta. Erityisesti työvälineiden ja henkilökohtaisten laitteiden ristiinkäyttöä kritisoitiin.

> -- mä koen, että se [tietoturva] on myös jollain tasolla tavallaan työnantajan vastuulla. Se, että ne laitteet on turvallisia ja ne mahdollistaa tietoturvallisen toimitustyöskentelyn. Työnantaja tavallaan luottaa siihen ne [työvälineet ja henk. koht. välineet] on erillään. (Haastateltava 4)

Osaamiskokemuksia jakaessaan toimittajat kertoivat myös konkreettisia tarpeita ja toiveita ammattitaidon ja osaamisen parantamiseen. Toimittajilla on aineiston perusteella tarvetta tietoturvakoulutukselle laajemmassa kuvassa, mutta kaikki

haastateltavat toivat lisäksi esiin toiveita ja suoria tarpeita jollekin tietylle tarkemmalle osa-alueelle. Suojattu viestintä ja lähdesuoja korostuvat molemmat aineistossa:

> -- mun mielestä myös toimittajia olisi hyvä kouluttaa siinä, että minkälaisia eri keinoja on esimerkiksi vastaanottaa materiaalia, tietoja tai tekstiä tai kuvia tai videoita tai mitä tahansa niin, että lähettäjän henkilöllisyys ei vaarannu. (Haastateltava 4)

Toiveissa oli myös apukeinoja, esimerkiksi julkisesti helposti löytyvää ohjeistusta, joka olisi suunnattu nimenomaan tietolähteelle.

> -- Olisi aika hyvä, että medioilla olisi omilla verkkosivuillaan sellaiset rautalankaohjeet siitä, että miten jos haluat turvallisesti lähestyä, niin teen näin ja ota nämä asiat huomioon. (Haastateltava 3)

Vaikka toimittajat ovat työssään melko itsenäisiä, yleinen aineistossa esiintyvä teema on tietoturvaohjeistuksen sekä yhteisten pelisääntöjen luominen yksittäiselle työpaikalle tai jopa koko alalle. Tämä tarve kumpuaa toimitusten monenkirjavista tietoturvakäytännöistä ja näiden puutteista.

Kouluttautumiseen haastateltavat suhtautuivat hyvin suopeasti. Kenelläkään haastateltavalla ei ollut aiempaa koulutusta tietoturvaan liittyen opinnoista tai työelämästä.

Koulutuksen järjestäjän ei välttämättä tarvitse olla työantajana. Kouluttajiksi toimittajat ehdottivat muun muassa yhdistyksiä tai muita ulkopuolisia tahoja. Onnistuneen koulutuksen kriteerejä ovat seuraavat: se olisi räätälöity toimittajille, ei menisi liian yksityiskohtaiseksi ja sillä olisi merkitystä arjen työhön.

> -- toivon, että olisi suomenkielistä, selkeätä koulutusta tietoturvallisuusasiaan ja nimenomaisesti eri tasoisille henkilöille. Jonkin verran tietoturvaan perehtyneenä, niin tiedän, että pahimmillaan tällainen foliohattu-neuroottisuus voi mennä hyvinkin pitkälle, niinkin pitkälle, että siinä ei enää ole minkäänlaista kosketuspintaa todellisuuteen. Hyvä olisi toimittajalle räätälöity paketti. (Haastateltava 4)

4.3 Työnantajan rooli

Työnantajalla on tietoturvallisessa toimitustyössä merkittävä rooli, sillä työantaja tarjoaa puitteet ja välineet työntekoa varten. Näiden oletetaan aineiston perusteella olevan siinä kunnossa, ettei toimittaja kohtaa ainakaan kriittisiä tietoturvariskejä työtä tehdessään. Työantajan oletetaan osin tekevän automaattisesti toimet tietoturvallisen työn varmistamiseksi. Toisaalta taas haastateltavat korostavat omien taitojen ja asenteen tärkeyttä: paraskaan työväline ei toimi, jos sitä ei osaa käyttää.

Työantajia sekä kiitellään että kritisoidaan. Ruusuja monen työnantaja saa uusista työvälineistä ja tietoturvan parantamisesta viimeisten vuosien aikana. Aineiston perusteella maailmalla ja kotimaassa esiintyvistä tietorikkeistä ja -murroista keskustellaan avoimemmin.

Risuja taas tulee etäisestä IT-osastosta, joka hoitaa työvälineitä, mutta ei välttämättä tiedä, mitä toimituksen kenttätyöhön oikeasti kuuluu. Haastateltavat kertoivat it-osaston ja toimittajien välisestä ”kuilusta”.

> --en oo ihan varma, onko sillä tietoturvayksiköllä riittävää käsitystä siitä. millaisissa oloissa me työskennellään. (Haastateltava 2)

Lisäksi kritiikkiä saa tietoturvaohjeistuksen puute tai sen piilottaminen hankalaksi koettuun paikkaan, kuten intranetin syövereihin.

Tietoturvan tärkeydestä ollaan haastateltavien mukaan tietoisia organisaatiotasolla, mutta yksittäinen toimittaja ei välttämättä tiedä, mistä saa tai voi hakea apua ongelmatilanteissa, oli kyse sitten tietoteknisestä ongelmasta tai maalittamisen kohteeksi joutumisessa. Usein ratkaisuna on aineiston mukaan ottaa yhteyttä IT-osastoon, joka ei välttämättä ymmärrä tarpeen merkitystä toimittajalle. Yksi esille nostettu esimerkki kuvaa tilannetta, jossa toimittajalla ei ole välinettä tai taitoa ottaa vastaan materiaalia lähteeltä salatussa muodossa. Esimerkkinä tästä on esimerkiksi maailmalla suosittu SecureDrop -palvelu, jota moni suurempi yhdysvaltalaistoimitus käyttää.

> -- siinä olisi toimituksille organisaationa kehittämisen paikka, että luotaisiin toimintamenetelmiä tiettyihin hypoteettisiin tilanteisiin, että joku esimerkiksi haluaa antaa tietovuodon tai kertoa jotain tietoja, joiden päätymisestä minnekään muualle täytyy olla paremmin varautunut. (Haastateltava 4)

Työnantajalta toivottiin keinoja, jolla arkaluontoisten lähteiden kanssa voisi viestittää tietoturvallisesti – ja että työantajana ymmärtäisi tämän tarpeen merkityksen.

Toimittajan vastuuttamista tietoturva-asioissa toisaalta kritisoitiin haastatteluissa: toimittajalla olisi suotavaa olla perustaidot arjen tietoturvaan, mutta, mutta lopulta työnantaja tekee päätökset työvälineistä. Tämä herätti ristiriitaisia tuntemuksia:

> --työnantaja valitsee millaisia järjestelmiä käytetään ja muuta, niin ei siinä yksittäinen toimittaja pysty mihinkään vaikuttamaan. (Haastateltava 3)

Somehäirinnän ja maalitetuksi joutuneen toimittajan auttamiseen kaivataan aineiston perusteella lisää resursseja ja metodeja jo tilanteiden ollessa käynnissä. Kuten luvussa 6.1. todetaan, toimittajat kokevat henkilökohtaisuuksiin menevät uhat vakavasti.

Aineistosta löytyy selvä toive siitä, että työyhteisöllä ja esihenkilöillä olisi kykyä auttaa häirinnän ym. uhriksi joutunutta toimittajaa jo ennen kuin häirintä tai maalitus etenee liian pitkälle. Tämä siis kielii toiveesta varautumiseen ja ennakointiin.

Luottamus työantajan ja työntekijän välillä on yksi työsuhteen kulmakiviä. Pääsääntöisesti haastateltavat toimittajat ovat luottaneet työantajiensa ”hoitavan oman tonttinsa”, vaikka parannus- ja kehittämisehdotuksia suorastaan vilisee aineistossa.

Luottamukseen kuuluu myös aineiston perusteella se, että työnantaja luottaa työntekijöihinsä niin, ettei synny sisäistä valvontaa, joka olisi omiaan aiheuttamaan epäluottamusta työyhteisön sisällä.

> Ehkä arjen tasolla luotan siihen, että jos nyt kirjoitan sähköpostin jollekin toimittajalle, niin ei sitä kukaan siinä välissä lue, ei edes työnantaja. (Haastateltava 3)

Kaikki haastateltavat eivät kuitenkaan luota täysin työantajansa tietoturvatoimiin, vaikka niistä keskustellaan nykyään aiempaa enemmän. Epäluottamus kumpuaa konkretian, kuten sääntöjen, puutteesta. Aineistossa verrattiin toimitusta ja suurta kansainvälistä yritystä: jälkimmäisessä on selkeät säännöt, mitä esimerkiksi työtietokoneella saa tehdä ja mitä ei.

> -- siellä [toimituksessa] on nyt paremmin asiat mietittynä. Tuntuu, että nyt näistä asioista puhutaan enemmän ja näitä tietoturvapuolen ihmisiä ollaan nähnyt enemmän, mutta on kuitenkin vähän eri asia keskustella näistä asioista ja sitten jättää kuitenkin sen toimittajan varaan sen, että miten se toteuttaa niitä neuvoja. (Haastateltava 2)

5 JOHTOPÄÄTÖKSET

Tämän tutkimuksen tavoitteena on selvittää kahden tutkimuskysymyksen avulla sitä, miten suomalaiset toimittajat kokevat tietoturvan ja mahdolliset tietoturvauhat työssään. Ensimmäisessä alaluvussa käsittelen, sitä miten haastateltavat kokevat tietoturvan yleisellä tasolla. Mukana luvassa ovat havainnot lähdesuojan kaksisuuntaisuudesta sekä osaamisen teema, joka sisältää koulutustarpeiden käsittelyn. Toinen alaluku käsittelee kokemuksia ja mietteitä tietoturvauhkista.

5.1 Abstraktiutta, etäistä IT-osastoa ja kaksisuuntaista lähdesuojaa

Ensimmäinen tutkimuskysymys oli: *miten toimittajat kokevat tietoturvan osana työtään?* Haastatteluaineiston ja aiemman tutkimuksen myötä on selvää, että tietoturva koetaan toimittajien keskuudessa jokseenkin etäisenä. Kokemukset tietoturvasta kiteytyivät pitkälti uhkakuvien pohdintaan sekä osaamisen sekä välineellisten puutteiden ja tarpeiden määrittelyyn. Yksi toimittajan tärkein tietoturvaan liittyvä aihepiiri on lähdesuoja, joka nostettiin jokaisessa haastattelussa keskiöön: lähdesuojasta huolehtiminen oli jokaisen haastateltavan tärkein suojeltava asia.

Yksi selitys digitaalisen turvallisuuden kokemiselle abstraktina on tietoturvan kokeminen vähäisenä omassa työnkuvassa tai oman toimituksen turvallisuuskulttuurissa. Jos työnkuvaa ei koeta tarpeeksi tärkeänä tai toimittaja ei ole esimerkiksi tutkivan journalistin asemassa, mielikuvamalli uhkista ja niihin varautumisesta voi olla huomattavan heikko (Tsui & Lee, 2021). Tämän tutkimuksen tulokset tukevat tätä em. Tsuin ja Leen väitettä. Tietoturva itsessään selitettiin auki lähinnä teoreettisten uhkakuvien kautta, koska suorat kokemukset sekä koulutus tietoturvariskeistä tai uhkaavista tilanteista puuttuivat. Samankaltaista havaitsivat Tsui ja Lee (2021, s. 8): journalistit, joilla on ”heikko uhkatietoisuus” ymmärtävät

tietoturvauhkat omnipotentteina voimina, kuten valtiotahoina, joita vastaan toimittajat eivät voi taistella. Tämän tutkimuksen haastateltavat eivät myöskään aina kokeneet tekevänsä sellaista työtä, jossa tietoturvaan pitäisi kiinnittää erityistä huomiota – lähdesuojaa lukuun ottamatta. Tämä huomio on linjassa Henrichsenin (2020) ja Tsuin ja Leen (2021) havaintojen kanssa: mitä arkisempaa journalismia tehdään, sitä vähemmän toimittajat ovat aiemmissa tutkimuksissa antaneet arvoa tietoturvan parantamiselle. Suurimmalla osalla tämän tutkimuksen haastateltavista ei ollut taustaa tutkivasta tai vastaavasta syvälle pureutuvasta journalismista ja he näkivät työnsä vähäriskisenä, koska he eivät kokeneet olevansa erityisen tärkeitä kohteita. Tämä on siis yksi selittävä tekijä siihen, miksi suurin osa haastateltavien koetuista uhkakuvista on luonteeltaan teoreettisia, esimerkiksi yhteiskunnallisia tai valtiollisia. Myös vakoilun mahdollisuus, joka tuli ilmi aineostossa, on tuttu uhkateema aiemmasta tutkimuksesta (Crete-Nishihata ym., 2020). Tämä kertoo osaltaan siitä, kuinka yleisellä ja yhteiskunnallisella tasolla tietoturvauhkat koetaan kenttätyössä ainakin tämän tutkimuksen haastateltavien mukaan – yleistyksiä koko alalle tästä ei voida tietenkään vetää. Toisaalta Hiltusen (2020) mainitsemista ulkoisen vaikuttamisen keinoista, kuten verkkohyökkäyksistä, murtautumisyrityksistä tai sosiaalisen median profiileihin tunkeutumisesta ei haastatteluissa mainittu mitään omakohtaista kokemusta – jos näistä keskusteltiinkin, ne olivat teoreettisia pelkoja.

Miksi sitten aineistossa esiintyy paljon abstraktiutta ja kuvitteellisia uhkia? Eräs selitys voisi löytyä McGregorin ja Watkinsin (2016) kehittämän security by obscurity-mallista, jossa journalisteista voidaan luokitella omaksi ryhmäkseen he, jotka uskovat tekevänsä niin vähäriskistä työtä, että he kokevat tietoturvariskit merkityksettöminä. Tällä luokittelulla on paljon samaa kuin Tsuin ja Leen (2021) tutkimuksen annissa. Luokittelu ei suoraan kuitenkaan tarkoita sitä, että toimittajat olisivat välinpitämättömiä – kyse on enemmänkin tietämättömyydestä ja sen vaikutuksesta omiin asenteisiin. Tämän tutkimuksen haastateltavat eivät aineiston perusteella vaikuta välinpitämättömiltä, päin vastoin: ymmärrystä tietoturvaan tuntuu löytyvän, vaikka riskit nähdäänkin laajemman käsityksen kautta. Kun tämä edellä mainittu vähäriskisyysluokittelu koskee niin toimittajia kuin johtavassa asemassa olevia toimituksen henkilöitä, muodostuu riski sille, ettei kukaan toimituksessa ole kiinnostunut tietoturvan parantamisesta tai kehittämään omia tietoturvataitojaan. Spekuloiden voisi pohtia, onko kenenkään etu toimitusympäristössä, jos tietotekniset ja asenteelliset haasteet lakaistaan maton alle, jos niitä ei nähdä tärkeäksi omassa työssä? Väitän, että ei ole ja yhdyn samalla McGregorin ym. (2016, s. 432) päätelmiin siitä, että journalistit ovat valmiimpia hyväksymään uusia tietoturvavälineitä- ja käytäntöjä, jos he ymmärtäisivät työnsä konkreettiset riskit. Olennainen rooli tämän

muutoksen aikaansaamisessa on työnantajapuolella ja johtoportaalla, joiden tehtävänä olisi kannustaa, ei torpata, tietoturvan kehittämistä.
Merkittävä havainto tuloksista liittyy lähdesuojaan ja sen kaksisuuntaisuuteen. Tällä tarkoitetaan sitä, että lähdesuojasta huolehtiminen ja lähteen suojaaminen ei ole pelkästään toimittajan tai toimituksen vastuulla. Samoja havaintoja on tehty myös aiemmassa tutkimuksessa (esim. Bradshaw, 2017; Henrichsen, 2020; Lee & Heinrichs 2019; Watkins ym, 2017). Lähdesuoja itsessään oli nostettu tämän tutkimuksen haastateltavien puheissa korkeimmalle jalustalle ja syystäkin: pelko siitä, että lähdesuojalle tapahtuisi jotain – se murrettaisiin tai se murtuisi – oli yksittäisistä tietoturvaan liittyvistä kokemuksista aineiston herkin. Tämä eroaa esimerkiksi siitä, mitä Paul Bradshaw 'n (2017) tutkimuksessa, jonka kyselyissä ja haastatteluissa selvisi, että lähdesuoja ja lähteen kanssa suojattu viestintä ei kosketa yhtä suurella painoarvolla kaikkia toimittajia, esimerkiksi paikallistoimittajia (Bradshaw, 2017, s. 11). Samassa Bradshawn' tutkimuksessa on myös havaittu toimituskunnan huolestuttava reaktio, jossa lähteiden uskotaan olevan jo valmiiksi niin hyvin perillä tietoturvallisuudesta, että toimituksen ei tarvitsisi muuttaa käytöstään (Bradshaw, 2017, s. 11). Tästä päästään lähdesuojan kaksisuuntaisuuteen, eli siihen, että lähteen toivotaan olevan paremmin perillä tietoturvasta tai jopa oletetaan pystyvän tietoturvallisempaan kommunikaatioon kuin mitä toimittaja itse pystyy. Huomionarvoista on sekin, että muutama vuosi Edward Snowdenin tapauksen jälkeen yhdysvaltalaisten tutkivien journalistien näkemyksiä haavoittuvuudesta ja mahdollisia muutoksia tietoturvakäyttäytymisessä tutkittiin Pew Research Centerin ja Columbian yliopiston digitaalisen journalismin yhteistutkimuksessa (Holcomb ym., 2015). Toimittajien tietoturvakoulutuksesta saadut vastaukset kertovat karua tarinaa oppimattomuudesta: alle puolet (41 %) tutkimukseen osallistuneista toimittajista oli koskaan saanut koulutusta tai edes opastusta heidän itsensä tietoturvan tai lähdesuojan parantamiseen. Kolme neljäsosaa vastaajista kertoi, etteivät ole perehtyneet tai parantaneet tietoturvataitojaan oma-aloitteisesti (Holcomb ym., 2015) Vaikka Holcombin edellä mainittu tutkimus on tehty yhdysvaltalaisten tutkivien toimittajien näkökulmasta, peilautuu sen kiteytetty tulos myös tämän tutkimuksen tuloksista. Haastateltavista suurin osa ei ollut koskaan käynyt tietoturvakoulutusta ja huoli osaamisen puutteesta heijastui myös lähdesuojan turvaamiseen.

Tämän tutkimuksen haastateltavat toivoisivat, että lähteet ymmärtäisivät lähdesuojan merkityksen ja osaisivat tietoturvallisen viestinnän keinoja nykyistä paremmin. Tämä eroaa esimerkiksi Henrichsenin (2020) tutkimuksen tuloksista, jossa osa yhdysvaltalaistoimittajista näkee tietoturvallisen kommunikoinnin jopa liiallisena toimenpiteenä, kuten myös lähteen kouluttamisen toimittajan taholta (Henrichsen, 2020, s. 338–339). Myöskään Bradshaw'n (2017) tutkimuksen havaintoa toimituksen

välinpitämättömästä asenteesta lähdesuojaa kohtaan tämän tutkimuksen aineistosta ei löydy ja oikeastaan reaktio haastatteluissa on aivan toisella linjalla: lähdesuoja on tärkeääkin tärkeämpää. Tämä on huojentava ja positiivinen havainto. Kaksisuuntaisen lähdesuojan lisäksi lähteen tärkeydestä kertoo tuloksissa esitetty havainto siitä, että toimittaja ei välttämättä pysty lupaamaan lähteelle ehdotonta suojaa esimerkiksi valtiovetoisen tarkkailun tai tiedustelun vuoksi. Freja Wedenborg (2018) ottaa esiin myös työnantajan tarkkailun: onko lähdesuojan yksipuolisesta lupaamisesta hyötyä, jos lähteen työnantaja näkee työntekijänsä (tässä tapauksessa siis lähteen) sähköpostit (Wedenborg, 2018, s. 13)? Sama huoli tuli miltei sanatarkasti ilmi eräässä tämän tutkimuksen haastattelussa. Kuten Paul Lashmar (2017) on tutkimuksessaan todennut, journalistien pitäisi ymmärtää lähdesuojan nykyiset vaarat, kuten tiedusteluelinten ja valvontaorganisaatioiden aiheuttamat uhkat, mutta myös niiden vastakeinot: edelleen on mahdollista tavata lähde esimerkiksi parkkipaikalla tai kahvilassa ilman puhelimia (jäljittämisen vaara) tai lähettää kirjepostia, jos digitaalisen viestinnän tietoturva tai suojaus arveluttavat. Lähdesuojan ja tietoturvaymmärryksen välillä on positiivinenkin puoli, jonka Tsui ja Lee (2021) tuovat esille: parempi ymmärrys tietoturvariskeistä on parantanut toimittajien viestintää lähteille. Käytännössä siis ne toimittajat, jotka ymmärtävät tietoturvariskejä ja osaavat suojella itseään, pystyvät kommunikoimaan turvallisemmin lähteiden (ja kollegojen) kanssa (Tsui & Lee, 2021, s. 13).

Digitaalisen ajan lähdesuojakysymys on monimutkainen eikä oikeita vastauksia voi hakea pelkästään yhteen ongelmaan takertumalla. Kuten haastateltavat aineistossa antavat ilmi, riskit lähdesuojan paljastumiseen piilevät syvällä arkisen työn varjoissa, kuten turvattomassa viestimisessä ja arkaluontoisen materiaalin salassapidon ongelmissa. Näistä kumpuavat toimittajien kokemukset ovat negatiivisia: vuotavaksi tiedetty tai epäilty tietoturva luo toimittajille selvästi turvattomuuden tunnetta, joka näkyy epävarmuutena ja huolena aineistossa. Koulutustarpeissakin tietoturvaosaamisen parantaminen lähdesuojan parantamiseksi nousi suureen rooliin – ja samalla kerrottiin vielä toive työantajille sekä koko alalle, että tietoturvakäytäntöihin saataisiin yhteisiä pelisääntöjä. Keinoja ja vinkkejä ongelmiin kuitenkin löytyy. Haastateltavien kertomat omat arjen vinkit tietoturvan parantamiseksi ovat hyvin linjassa niiden kanssa, joita Julie Posetti (2017) tutkimuksessaan listaa: analogisten välineiden, kuten kynän ja paperin, käyttäminen tilanteen vaatiessa, yleisön opastaminen ja tiedottaminen turvallisista viestintäkäytännöistä- ja välineistä, tietoturvallisen kommunikaation tärkeyden täsmentäminen yleisölle ja lähteille sekä mahdollisten kolmannen osapuolen, kuten järjestöjen, ottaminen mukaan opastamaan ja kouluttamaan toimituksia. Tässä listauksessa on mukana jo siis muutakin kuin yöllisiä parkkipaikkakohtaamisia.

Kuten osa haastateltavistanikin ehdottivat, Posettikin (2017) korostaa vinkeissään lähteiden oman tietoturvaosaamisen parantamista. Tämä tarkoittaa lähdesuojan merkityksen sanallistamista julkisesti sekä lähteiden suoranaista opastamista digitaalisissa uhkissa (Posetti, 2017, s. 138).

Osaamisen ja omien taitojen kokemusta ei tässä tutkimuksessa voi sivuuttaa. Haastateltavien vastauksista korostunut hämmennys omien taitojen sanoittamisesta, yksilön toimintamallien puute, organisaatioiden tekemien päätösten hallitsemattomuus ja toimittajan tekemät tietoturvakompromissit kertovat siitä, kuinka pienenä tekijänä yksittäinen toimittaja kokee itsensä työn virrassa. Vaikka mitään tämän tutkimuksen tulosta tai johtopäätöstä ei voida viedä sellaisenaan koko mediakenttää kattavaksi tulkinnaksi, on selvää, että huolta toimittajien joukossa herättää erityisesti puutteet tietoturvataidoissa. Jos uhkat nähtiin abstrakteina, puutteet omissa (ja kollegoiden) taidoissa ovat konkreettisia: vahvuuksia ei tunnu löytyvän esimerkiksi ohjelmistojen käytössä tai tietoturvallisessa viestinnässä. Teknologista puolta katsoen haastateltavat kuitenkin ymmärsivät sosiaalisen median ja tiettyjen viestintävälineiden, kuten WhatsAppin, tietoturvariskit. Osa oli siirtynyt käyttämään esimerkiksi toimittajien keskuudessa suosittua Signal-sovellusta. Yleisesti uhkaavana koettiin hallitsematon tilanne, joka tulee eteen yllättäen ja toimittaja joutuu reagoimaan siihen omien taitojensa mukaan. Taidot linkittyvät myös osaltaan Tsuin ja Leen (2021) mielikuvamalleihin, jotka erään haastateltavan tapauksessa tulivat esille parempina koettuina taitoina – rikosuutisoinnin parissa työskentely toi toimittajalle paremman kuvan omasta osaamistasosta. Tästä voidaan vetää johtopäätös, että parempi varautuminen edes ajatuksen tasolla potentiaalisiin uhkiin voi parantaa myös tietoturvataitojen hallitsemisen kokemusta. On tietenkin mahdotonta sanoa, parantaako syvemmälle pureutuvampi työnkuva tietoturvataitoja, mutta sillä voi ainakin spekuloida ajatuksen tasolla. Aiheen syvällisempi jatkotutkimus on mielestäni tärkeää, sillä jos toimittajien mielikuvia työnsä merkityksestä voidaan parantaa, voi sillä olla positiivisia seurauksia myös siihen, millaiset taidot koetaan merkityksellisinä.

Lisäkoulutus ja osaamisen lisääminen korostuivat haastatteluissa positiivisessa mielessä. Aiemman osaamisen parantaminen konkreettisen koulutuksen avulla koettiin mielekkäänä. Tämä toisi yksilön lisäksi koko yhteisölle parempaa osaamista. Se, että koulutus olisi räätälöity erityisesti toimittajia varten, kertoo siitä, että toimittajat arvostavat alan standardien tuntemista ja oman työn kipupisteisiin paneutumista. Ennen kaikkea koulutustoiveet kertovat motivaatiosta oppia uutta – samoin kuin kommentit pohtia tietoturvaa uusin silmin tämän tutkimuksen virittämänä.

Työantajien rooli aineistossa on kaksijakoinen. Työantajia kehutaan tietoturvan nostamisesta keskustelun tasolle, mutta haasteita löytyy erityisesti johtoportaan asenteista tietoturvan tärkeyttä kohtaan sekä erityisen leveänä koetusta kuilusta toimittajien ja toimitusten IT-osaston välillä. Lisäksi haastateltavat kritisoivat työnantajia siitä, että tärkeä tietoturvaohjeistus oli joissain tapauksissa piilotettu esimerkiksi intranetin syvyyksiin. IT-osaston etäisyydestä kertoo erään haastateltavan kommentti siitä, että hän ei ole varma ymmärtääkö IT-osasto aina toimittajien työtä ja journalismin tarpeita. Tämä kokemus on yhteneväinen Henrichsenin (2020) ja Watkinsin ym. (2017) tutkimusten havaintojen kanssa. Tämän tutkimuksen haastateltavien kokemukset IT-osaston kaukaisuudesta kumpuavat epävarmuudesta ja osittain myös luottamuksen puutteesta IT-osaston, johdon ja toimittajan välillä – kun ei puhuta ”samaa kieltä”, tavoitteita ja tarpeita ei saada sanoitettua. Crete-Nishihata ym. (2020) nostavat esille turhautumisen, joka kumpuaa IT-osaston ”yhteyden katkeamisesta” toimituksen kanssa, joka voi pahimmillaan johtaa siihen, että IT-osasto on suurin este tietoturvametodien käytössä esimerkiksi estämällä tarvittavien ohjelmistojen asennuksen (Crete-Nishihata ym. 2020, s. 1081). Kompromissit ovat osa työelämää, mutta haastatteluissa selvisi, että osa toimittajista kokee olevansa vastuussa tietoturvasta ja sen käytön hallinnasta, mutta työnantaja tekee loppupeleissä päätöksen, miten ja millä välineillä tietoturvasta huolehditaan. Tällainen menettelytapa on omiaan aiheuttamaan sekavuutta ja kaaosta organisaatiossa. Watkins ym. (2017) väittävätkin tutkimuksessaan, että tällainen sekavahko toimintamalli voi vaarantaa yksilön lisäksi koko organisaation tietoturvan. Tämän tutkimuksen haastateltavan huoli on yhteydessä jo aiemmin mainittuun toimittajan autonomisen työn kulttuuriin, joka näyttäytyy nyt myös painavana vastuuna, mutta ristiriitaisena sellaisena: millä tavoin toimittaja voi toimia ”oikein”, jos vaakakupissa ovat oma ammattitaito sekä työnantajan asettamat velvollisuudet , ehkä myös esteet. Kuten Henrichsen (2020) toteaa, johdon ja toimituksen välillä on ristiriitaa ja ymmärtämättömyyttä: johtoporras ei aina tunnu ymmärtävän, miksi toimittaja käyttää aikaa vieviä tietoturvamenetelmiä, vaikka jutun voisi tehdä nopeamminkin. Tästä voi seurata se, että jutun valmistuminen on tärkeämpää kuin sen tekeminen tietoturvallisesti (Henrichsen, 2020, s. 7). Työnantajakokemukseen vaikuttaa myös maine ja sen menettämisen pelko. Kaksi haastateltavista otti esiin huolestuttavana julkisuusesimerkkinä Helsingin Sanomien tapauksen, jossa toimittaja yritti tuhota tietokonettaan vasaralla tietoja tuhotakseen. Julkisuuskuvan ja maineen menettäminen ollut työnantajien ja toimittajien huolena jo aiemmassa tutkimuksessa (esim. Watkins & Anderson, 2019, s. 15; McGregor ym., 2016, s. 424) Tämä kertonee siitä, että toimittajakunta haluaa suojella mainettaan yleisön silmissä

esimerkiksi lähteiden menettämisen pelossa, jota muun muassa Lashmar (2017) on tutkinut.

Työantajakysymykseen liittyy myös työsuhteen tyyppi ja sillä näyttääkin olevan vaikutusta siihen, miten hyvin tai huonosti tietoturvassa onnistutaan. Crete-Nishihata ym. (2020) toteavat, että freelancer-toimittajilla on autonomisen työnsä vastapainona heikompi tietoturvan ymmärrys ja toimintamallit. Syitä tähän ovat esimerkiksi rahan puute, organisaation tuen ja myös sääntöjen puuttuminen sekä yksinkertaisesti resurssien puute – freelancer huolehtii yksin kaikesta eikä hänellä yleensä ole erillistä IT-osastoa tukenaan. Yleisesti katsoen määräaikaista tai kokoaikaiseksi katsottua työtä tekevällä toimittajalla on jonkinlainen organisaatio ja myös sen tuoma taloudellinen taustakehys. (Crete-Nishihata ym., 2020) Tämän tutkimuksen aineistossa freelancereiden tietoturva tuli ilmi vain kerran, mutta sitäkin ytimekkäämmin. Haastateltava näki ristiriidan freelancerin ja ”talon sisäisen toimittajan” välillä: on freelancerista itsestään kiinni, onko hänellä virustorjunta, palomuuri tai VPN-yhteys. Kyse on yhtä lailla osaamisesta, kiinnostuksesta ja rahasta. Voidaan siis sanoa, että tietoturvan sälyttäminen pelkästään freelancerin harteille on melkoinen riski toimitusorganisaatiolle.

Toivelista työnantajille tämän tutkimuksen toimittajilta pitää sisällään kiteytetysti seuraavat asiat: parempi kommunikaatio johdon, toimituksen ja IT-osaston välillä, tietoturvakoulutuksen selvä lisääminen, selvät toimintamallit tietoturvaan liittyvien ongelmatilanteiden lisäksi myös häirintätilanteiden hoitoon jo niiden alkuvaiheessa. On helppo yhtyä Watkinsin ja Andersonin (2019) vinkkeihin työnantajille siitä, miten toimitusten tietoturvaa (ja samalla diversiteettiä) voi parantaa: palkataan ihmisiä eri taustoilla ja työkokemuksilla. Voimavaraa voi toimitukseen tulla hyvinkin siitä, että eri aloja tuntevat ihmiset työskentelevät yhdessä (Watkins & Anderson, 2019). Aihepiirinä työnantajaa koskeva kokonaisuus on mielenkiintoinen, koska se pitää sisällään kaksi toimijaa, alaiset ja johdon. Aihe vaatisi ehdottomasti lisätutkimusta kotimaisella mediakentällä.

5.2 Suurimpina pelkoina häirintä ja toimintakyvyttömäksi tekeminen

Toisena tutkimuskysymyksenä oli: *millaisia tietoturvauhkia toimittajat kokevat työssään*. Aineisto tarjoaa kattauksen toimittajan tietoturvauhkia, joita haastateltavat pääasiassa spekuloivat peilaten omaan työkokemukseensa. Kuten jo aiemmassa alaluvussa on todettu, pääkokemukset tietoturvasta kiteytyivät lähinnä uhkakuviin. Tässä

alaluvussa pureudutaan kuitenkin entistä tarkemmin niihin uhkiin, jotka nostin esille aineistosta ja joita peilaan alan aiempaan tutkimukseen. Mukana on abstraktien mielikuvien lisäksi konkretiaa, kuten somehäirintää ja maalittamista. Aineisto tarjoaa toiseen tutkimuskysymykseen huomattavasti suppeammin materiaalia, josta johtuu myös tämän alaluvun selvä lyhyys verrattuna edeltävään.

Vaikka aiemman alaluvun alussa mainittiinkin aineistossa esiintyviksi tietoturvauhkiksi abstraktimmat asiat, kuten valtiotahojen tekemä vakoilu, suurin rooli haastateltavien kokemissa uhkissa on kuitenkin arjen konkretiassa. Merkittävimmät tuloksista nostamani asiat liittyvät joko toimitukseen tai toimittajaan itseensä kohdistuviin suoriin uhkakuviin. Näistä kaksi merkittävintä ovat sosiaalisen median häirintä ja maalittaminen. Yhteisenä nimittäjänä näille uhkille on niiden henkilökohtaisuus: niissä taho, oli se sitten valtio tai yksittäinen ihminen, saa käsiinsä tietoa, jolla voisi uhata toimittajaa tai jopa hänen lähipiiriään. Myös henkisesti toimintakyvyttömäksi joutuminen tällaisen iskun jälkeen on konkreettinen huoli. Tällainen maalittaminen tai häirintä voi tulla yksityisiltä henkilöiltä, mutta myös erilaisilta joukkioilta ja ryhmittymiltä. Toimittajien häirinnästä laajan tutkimuksen tehnyt Silvio Waisbord (2020) toteaa moninaisen toimittajiin kohdistuvan häirinnän olevan ainakin Yhdysvalloissa yleistynyt ilmiö, johon kuuluvat lehdistön trollaamisen lisäksi uutena ilmiönä *mob censorship*, joka vapaasti suomennettuna tarkoittaisi joukkosensuuria. Siinä journalismia ja sen tekijöiden sananvapautta yritetään vaientaa verkon eri kanavien kautta tapahtuvalla häirinnällä, jonka Waisbord rinnastaa vihapuheeseen. Häirintä onkin johtanut yhdysvaltalaistoimittajilla moninaisiin ongelmiin, kuten traumoihin, tunne-elämän stressiin, motivaation katoamiseen ja jopa alanvaihtoajatuksiin (Waisbord, 2020, s. 8–11). On kuitenkin tärkeää erottaa häirintä journalistisesta palautteesta, joka on usein suoraviivaista ja voi kohdistua suoraan toimittajan persoonaan kärkkäästikin. Häirintä itsessään on vahingollista ja sitä voi esiintyä monissa muodoissa, kuten aineistostakin ilmenee. Digitaalisen työympäristön häirintä on aiemmassa tutkimuksessa esiintynyt esimerkiksi nykyään valitettavan tavanomaisina uhkaavina viesteinä tai henkilökohtaisen tiedon levittämisenä (esim. Crete-Nishihata, 2020, s. 1079). Toisaalta voi pohtia sitä, onko hyökkäyksen kohteeksi joutumisesta mitään hyötyä. Yksi mahdollisuus on se, että hyökkäyksen kohde jakaa kokemustaan ja oppejaan aiheesta työympäristössä kollegoilleen (Henrichsen, 2021). Tämä voi olla kullanarvoista ensi käden tietoa tapahtuneesta ihmisille, jotka eivät ole kokeneet vastaavaa ja voi auttaa toimittajakollegoita ja työympäristöä varautumaan tietoturvaan ja persoonaan kohdistuviin hyökkäyksiin. Tämä ei tietenkään poista työantajan roolia toimia häirintää kokeneen toimittajan ensisijaisena auttavana kätenä eikä etenkään sitä, että toimittajien häirintä pitäisi saada loppumaan tyystin.

Yksi johtopäätös tuloksista on työn ja vapaa-ajan lomittumisen mukanaan tuomat uhkakuvat. Vaikka tämän tutkimuksen pääfokus ei olekaan vapaa-ajan tutkimisessa, tuloksista selviää, että digitaalisessa työssä myös henkilökohtaisilla laitteilla ja yksilön toimintatavoilla on merkitystä. Aiemmassa tutkimuksessa (esim. Haag & Eckhardt, 2014; Rentrop & Zimmermann, 2012) työntekoa henkilökohtaisilla välineillä kutsutaan uudehkolla termillä ”varjo-IT”. Termi esiintyy tulkintani mukaan tämän tutkimuksen tuloksissa siten, että haastateltava on esimerkiksi käyttänyt omaa älypuhelinta työtehtävissä ilman työnantajan lupaa. Tietoturvariskin muodostaa juuri tiedostamattomuus: työnantaja ei voi tarjota tietoturvaa laitteelle, josta ei tiedä mitään. Haastateltavat, jotka kertoivat oman laitteen käytöstä, tiedostivat käsitykseni mukaan viimeistään haastattelutilanteessa omien laitteiden riskit työssään. Eräs haastateltavista totesikin osuvasti, että oma puhelin on täysin toimittajan itsensä varassa. Journalismin ja henkilökohtaisten työvälineiden osalta tilanne vaikuttaa loppujen lopuksi huolestuttavalta: autonomisen työnkuvan ansiosta, tai pakosta, toimituksissa yksilöt tekevät aineiston ja tutkimusten perusteella edelleen päätöksiä itsenäisesti eikä IT-osaston tai johdon suoria määräyksiä lukuun ottamatta kukaan tunnu hallitsevan pehmeämpää tietoturvaosaamista, kuten asenteita ja koulutusta. Tämä ei pelkästään siis koske varjo-IT:tä, vaan koko asetelma peilautuu laajemmin toimituksiin, osaamispulaan ja asenneongelmiin. Yksi ja samalla kenties eksoottisin varjo-IT:tä sivuava aihe on aineistossa esiintyvä yksityisyyden menettäminen käyttäjää seuraavia appeja, kuten urheilusuorituksia mittaavan Sports Trackeria käyttämällä. Vastaavien applikaatioiden ja sovellusten tietoturvauhka ja -riski piilee siinä, että palvelut julkistavat usein käyttäjän ”tuloksia”, kuten juoksulenkkejä ja niiden reittejä, julkiselle verkkosivulle. Teoriassa tätä kautta on mahdollista seurata toimittajan liikkeitä hyvinkin reaaliajassa ja yhdistää lankoja – ketä on tavattu, miksi on liikuttu missäkin. Vaikka asetelma kuulostaa kevyehkön agenttielokuvan sivujuonelta, riski esimerkiksi lähteen paljastumiselle seurantatietoja tutkimalla on todellinen – onhan jo pelkästään puhelimen paikantaminen tukiasemien kolmiomittauksella ollut mahdollista jo pitkään. Pohdittavaksi jää, että voisiko varjo-it:stä olla hyötyä toimittajan työssä. Aiemman tutkimuksen perusteella voi todeta, että tällä hetkellä varjo-it:n tutkimuksessa keskitytään suurelta osin sen tuomiin negatiiviisiin vaikutuksiin, kuten tietoturvariskeihin. Yksi varteenotettava mahdollisuus henkilökohtaisen ja työteknologian risteyttämisessä voisi olla teknologian nopeampi oppiminen: ne, jotka osaavat käyttää uusia laitteita käyttäisivät niitä myös työssä. Tämä toisi alalle kauan kaivattua uusien teknologioiden haltuunottoa, jossa toimittajat alana tuntuvat olevan hieman jälkijunassa. Tämän tutkimuksen haastatteluista kumpuaa myös eräänlainen kritiikki työnantajan tarjoamia välineitä kohtaan: ne ovat ylhäältä annettuja eikä niitä aina koeta uusimpina

ja turvallisimpina. Sama turhautuminen on tuotu esiin Haagin ja Eckhartin (2014) tutkimuksessa: työn tehokkuutta vaalivassa kulttuurissa mikä tahansa työympäristössä tehoa rajoittava tekijä koetaan ”turhauttajana” ja siitä voidaan pyrkiä eroon tekemällä työtehtävät tutuiksi koetuilla välineillä ja metodeilla. Henkilökohtaisesti pidättäydyn suosittelemasta henkilökohtaisten välineiden käyttöä journalistisissa työprosesseissa – tietoturva on mielestäni tärkeämmässä roolissa.

Tietoturvauhkiin, kyberhyökkäyksiin ja toimitustyön tietoturvariskeihin liittyy niiden tunnistaminen. Tosiasia kuitenkin on, että harva ihmisistä pystyy tunnistamaan verkkohuijauksen silmänräpäyksessä – ne kun tehdään usein silmiltä piilossa tai niin vakuuttavasti, että ne eivät herätä erityistä huomiota. On siis ymmärrettävä, että yksittäinen toimittaja ei välttämättä tunnista kyberuhkaa tai suoraa hyökkäystä. Hiltunen (2020) toteaakin tutkimuksessaan, että verkkohyökkäykset saattavat kohdistua toimittajan sijaan koko organisaatioon ja tällaisen hyökkäyksen tunnistaminen edellyttää laajaa tietoteknistä osaamista (Hiltunen, 2020, s. 199). Tällainen tietotekninen osaaminen vaatisi joko vahvaa harrastuneisuutta tai ammattitaitoa ja voidaankin pohtia, monestako suomalaisesta toimituksesta löytyy yksilöitä, jotka ovat IT-taidoiltaan vahvoilla. Tähän aiheeseen olisi hyvä hakea vastauksia jatkotutkimuksen avulla toimittajien taitoja tutkien.

6 PÄÄTÄNTÖ

Tutkimuksen loppuluvussa käyn ensin läpi työn arvioinnin. Toisessa alaluvussa pohdin syvällisemmin tutkimuksen kahta päähaastetta. Lopuksi vedän yhteen jatkotutkimusideoita, joita en ole käsitellyt aiemmassa Johtopäätökset-luvussa.

6.1 Tutkimuksen arviointi

Tämän tutkimuksen aihepiiri on laaja eikä kotimaista tutkimusta siitä ole vielä tehty. Kaikki tämä aiheutti runsaasti haasteita tutkimuksen alusta loppuun: miten tutkimus toteutetaan, onko rajaus tarpeeksi tiukka, onko valittu analyysimenetelmä oikea, onko haastateltavien joukko tarpeeksi suuri ja monipuolinen, miten tutkija itse suhtautuu aiheeseen ja onko tällä kaikella vaikutusta lopputulokseen. Lisäksi haastattelumetodin valinta herätti ajatuksia: olisiko tutkimuksesta tullut kattavampi, jos metodiksi olisi valittu kysely? Kysymysmyrskystä huolimatta kokonaiskuvasta rakentui objektiivinen, vaikkakin hieman suppea katsanto aiheeseen suomalaisten toimittajien äänillä. Tutkimusta arvioidessa on tärkeää ottaa huomioon vahvuudet ja heikkoudet. Ehdottomana vahvuutena näen tutkimuksen aiheen ainutlaatuisuuden ja ajankohtaisuuden sekä ainestonkeruun menetelmät, jotka antavat haastatteluiden ansiosta luettavaksi tärkeittä katkelmia haastateltavien puheesta. Haastateltavat eivät myöskään edusta pelkästään yhden työantajan väkeä ja tavoitteeni haastateltavien diversiteetistä onnistui tältä osin. Suurimpana heikkoutena näen haastateltavien suhteellisen pienen määrän ja sen, että he edustavat anonyymeinakin vain henkilökohtaista kantaansa eikä tästä tutkimuksesta voi vetää suoria johtopäätöksiä koko Suomen mediakenttään.

Haasteensa tämän tutkimuksen tieteelliselle arvioinnille asettaa sen tyyppi laadullisena tutkimuksena. Jari Eskolan ja Juha Suorannan (2015) mukaan

luotettavuus on yksi laadullisen tutkimuksen arvioinnin mittareista, mutta toisin kuin määrällisessä tutkimuksessa, laadullisessa tutkimuksessa on mahdollista kulkea vapaasti analyysin, tulkintojen ja tutkimustekstin välillä. Tutkija joutuu pohtimaan ratkaisujaan ja näin ottamaan kantaa työnsä luotettavuuteen. Tutkijan on syytä myös tiedostaa olevansa itse luotettavuuden mittari – tämän myötä luotettavuuden arviointi tulee parhaiten esiin siinä, miten tutkimusprosessia on kuvattu ja avattu. Avoimuus on tärkeää, ja siihen olen pyrkinyt tämän työn kaikissa vaiheissa. Neljä avainkäsitettä, *uskottavuus, siirrettävyys, varmuus* ja *vahvistuvuus* koskevat olennaisesti luotettavuuden määritelmää (Eskola & Suoranta, 2015, s. 321–327; Tuomi & Sarajärvi, 2018, s. 114–115). *Uskottavuudella* tarkoitetaan sitä, miten tutkija pystyy varmistamaan sen, että hänen ja tutkittavien käsitykset vastaavat toisiaan. *Siirrettävyydellä* tarkoitetaan taas sitä, että tutkimuksen tulokset ovat mahdollisesti siirrettävissä toiseen kontekstiin tietyin ehdoin. *Varmuudella* tarkoitetaan sitä, että tutkija ottaa huomioon tutkimukseen vaikuttavat, ennustamattomat tekijät. *Vahvistuvuudella* taas haetaan sitä, että tutkijan tulkintaan voidaan saada tukea esimerkiksi saman aiheen aiemmasta tutkimuksesta. (Eskola & Suoranta, 2015, 326–327). Luotettavuuden osalta tässä tutkimuksessa olen pyrkinyt tuomaan esiin nimenomaan tutkittavien kokemuksia aiheesta varmistamalla haastatteluissa, että puhumme samasta asiasta. Tässä minua auttoi journalistinen taustani, joka auttoi havainnoimaan mahdollisia tarkennusta vaativia kohtia haastattelutilanteissa. Vahvistuvuus täyttyy tämän tutkimuksen osalta sillä, että tulkintaan ja johtopäätöksiin on saatu vahvistus aiemmasta tutkimuksesta, joka omalta osaltaan on täydentänyt tämän työn merkittävyyttä. Uskottavuuden parhaaksi mittariksi tässä työssä lasken sen, miten avoimeksi olen itse tutkimuksen ja sen raportoinnin rakentanut. Tärkeimpiä huomioita näistä ovat perin pohjin avatut haastateltavien valintaprosessi, haastattelumetodi ja analyysin työkulku. Lisäksi halusin tuoda tulosluvussa haastateltavien suoria sitaatteja lukijan arvioitavaksi. Näin viimeinen päätös tämän tutkimuksen aineiston luotettavuudesta on lukijalla, joka tekee omat johtopäätöksensä lukemansa perusteella.

6.2 Liian vähän haastateltavia tai faktojen silottamista?

Kaksi tämän työn päänvaivaa aiheuttanut haastetta olivat mielessäni jo tutkimuksen alkuvaiheilla. Ne olivat tutkijan epävarmuus siitä, saanko tutkimukseen tarpeeksi osallistujia ja faktojen silottamisen mahdollisuus tutkimusaiheessa, joka on arkaluontoinen. Ensimmäinen ongelma väistyi onneksi ensimmäisten tutkimusviikkojen aikana haastateltavien suostuttua tutkimukseen, mutta toinen epävarmuustekijä on vaivannut loppuraportin kirjoittamiseen asti. En halua, enkä

voi, esittää epäluottamusta tutkimukseen osallistuneita kohtaan, mutta tutkimusta kohtaan pitää mielestäni esittää tervettä kritiikkiä: en voi piilottaa sitä häviävän pientä mahdollisuutta, että anonymiteetin turvinkaan tietoturva-aihe olisi tämän tutkimuksen myötä käsitelty pahimpien mahdollisten kokemusten tai skenaarioiden kautta. Kysymykseni on siis: sanottiinko kaikki silottelematta? Toivottavasti sanottiin. Voin vain toivoa ettei alalla ei esiinny pahempia esimerkkejä tietoturvaan liittyvistä asenteista tai riskeistä, mutta tämän toteaminen ilman tarpeellista jatkotutkimusta on vain spekulaatiota.

6.3 Jatkotutkimusideoita

Tietoturvan ja journalismin suhde antaa kotimaisittain ja kansainvälisesti hyvän pohjan jatkotutkimukselle, josta useasta voisi koitua konkreettista hyötyä koko alalle.

Johtopäätöksissä esitettyjen jatkotutkimusaiheiden lisäksi journalismin tietoturva kaipaisi lisätutkimusta erityisesti työnantajapuolen sekä IT-osaston kokemuksia tietoturvasta. Aiemmassa tutkimuksessa perehdytään joissakin määrin toimitusorganisaatioiden yleisiin kokemuksiin (esim. McGregor ym., 2016), mutta kotimaiselta kentältä tämä puuttuu täysin. Jatkotutkimus organisaation näkökulmasta voisi tuoda alalle kaivattua läpinäkyvyyttä myös pöydän toiselta puolelta ja omalta osaltaan ehkäistä johdon, toimituksen sekä IT-osaston välille syntyviä kuiluja.

Tämän tutkimuksen johdosta olisi myös tärkeää selvittää, millainen suomalaisten toimittajien kanta tietoturvateknologioihin ja niiden käyttöön on. Tämän tutkiminen tuo uutta näkökulmaa siihen, mitkä asiat mahdollisesti motivoivat kotimaisia toimittajia parantamaan omaa tietoturvaansa. Samalla olisi mielenkiintoista tutkia sitä, esiintyykö toimituksissa Henrichsenin (2021) mainitsemia ”tietoturvan esitaistelijoita” ja jos, mikä heidän roolinsa työorganisaatiossa on.

Varjo-IT:n osalta jatkotutkimusta voisi toteuttaa usealtakin osa-alueelta: siitä, miten yleistä omien laitteiden ja välineiden käyttö on toimitustyössä, miten johto tai IT-osasto (erikseen) suhtautuvat niiden käyttöön ja ymmärtävätkö toimittajat itse henkilökohtaisten välineiden käytön riskit.

Tämän tutkimuksen yksi aineistonkeruumenetelmä olisi voinut olla kysely ja pohdinkin päätteeksi sitä, josko laajalla kyselyllä tietoturva-journalismiaiheesta saisi vieläkin kattavamman kuvan kotimaisen kentän osaamisesta ja asenteista.

VIITTEET

Bradshaw, P. (2017). Chilling Effect: Regional journalists' source protection and information security practice in the wake of the Snowden and Regulation of Investigatory Powers Act (RIPA) revelations. *Digital Journalism*, *5*(3), 334–352. https://doi.org/10.1080/21670811.2016.1251329

Crete-Nishihata, M., Oliver, J., Parsons, C., Walker, D., Tsui, L., & Deibert, R. (2020). The Information Security Cultures of Journalism. *Digital Journalism*, *8*(8), 1068–1091. https://doi.org/10.1080/21670811.2020.1777882

Di Salvo, P. (2021). Securing Whistleblowing in the Digital Age: SecureDrop and the Changing Journalistic Practices for Source Protection. *Digital Journalism*, *9*(4), 443–460. https://doi.org/10.1080/21670811.2021.1889384

Eskola, J., Suoranta J. (1998). *Johdatus laadulliseen tutkimukseen*. Vastapaino. Päivitetty e-kirja 2015, haettu palvelusta Storytel 28.4.2022

Haag, S., & Eckhardt, A. (2014). Normalizing the Shadows – The Role of Symbolic Models for Individuals' Shadow IT Usage. *Thirty Fifth International Conference on Information Systems*, *2014*, 13.

Henrichsen, J. R. (2020). Breaking Through the Ambivalence: Journalistic Responses to Information Security Technologies. *Digital Journalism*, *8*(3), 328–346. https://doi.org/10.1080/21670811.2019.1653207

Henrichsen, J. R. (2021). Understanding Nascent Newsroom Security and Safety Cultures: The Emergence of the "Security Champion". *Journalism Practice*, 1–20. https://doi.org/10.1080/17512786.2021.1927802

Hirsjärvi, S. & Hurme, H. (2001). Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. Helsinki: Helsinki University Press

Hiltunen, I. (2020). Ulkoinen vaikuttaminen ja sen vastakeinot suomalaisessa journalismissa. *Media & viestintä*, *43*(3). https://doi.org/10.23983/mv.98406

Holcomb, J., Mitchell, A., & Page, D. (2015). Investigative Journalists and Digital Security: Perceptions of Vulnerability and Changes in Behaviour. *Pew Research Center in Association with Columbia University's Tow Center for Digital Journalism*, 18.

Jaakkola, M. (2013). *Hyvä journalismi: Käytännön opas kirjoittajalle*. Kansanvalistusseura.

Jansson, S., & Sihvonen, T. (2018). Kyberturvallisuus valtiollisena toimintaympäristönä ja siihen kohdistuvat uhkat. *Media & viestintä*, *41*(1). https://journal.fi/mediaviestinta/article/download/69950/31049

Kallinen, Timo & Kinnunen, Taina. Etnografia. Teoksessa eri toimittajia (mainittu viitteen yhteydessä). Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. Haettu osoitteesta https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus. Viitattu 30.11.2021

Kirchgaessner, S., Lewis, P., Pegg, D., Cutler, S., Lahkani N. & Safi, M. (18.7.2021) *Revealed: leak uncovers global abuse of cyber-surveillance weapon*. The Guardian. https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

Huoltovarmuuskeskus. (2018) *Kyberturvallisuuden sanasto*. Sanastokeskus TSK ry. https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Lashmar, P. (2017). No More Sources?: The impact of Snowden's revelations on journalists and their confidential sources. *Journalism Practice*, *11*(6), 665–688. https://doi.org/10.1080/17512786.2016.1179587

Lee, M., & Heinrichs, R. (2019). *How to protect the truth? Challenges of cybersecurity, investigative journalism and whistleblowing in times of surveillance capitalism. An interview with Micah Lee*. 18.

McGregor, S. E., Roesner, F., & Caine, K. (2016). Individual versus Organizational Computer Security and Privacy Concerns in Journalism. *Proceedings on Privacy Enhancing Technologies*, *2016*(4), 418–435. https://doi.org/10.1515/popets-2016-0048

Posetti, J. (2017). *Protecting journalism sources in the digital age*. http://unesdoc.unesco.org/images/0024/002480/248054E.pdf

Rentrop, C., & Zimmermann, S. (2012). *Management and Control of unofficial IT*. 6.

Tuomi, J., & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi.* Kustannusosakeyhtiö Tammi.

Wahl-Jorgensen, K., Bennett, L. K., & Cable, J. (2017). Surveillance Normalization and Critique: News coverage and journalists' discourses around the Snowden revelations. *Digital Journalism*, *5*(3), 386–403. https://doi.org/10.1080/21670811.2016.1250607

Waisbord, S. (2020). Mob Censorship: Online Harassment of US Journalists in Times of Digital Hate and Populism. *Digital Journalism*, *8*(8), 1030–1046. https://doi.org/10.1080/21670811.2020.1818111

Watkins, E. A., Al-Ameen, M. N., Roesner, F., Caine, K., & McGregor, S. (2017). *Creative and Set in Their Ways: Challenges of Security Sensemaking in Newsrooms*. 12.

Watkins, E. A., & Anderson, C. W. (2019a). Managing journalistic innovation and source security in the age of the weaponized Internet. Teoksessa A. L. Bygdås, S. Clegg, & A. L. Hagen (Toim.), *Media Management and Digital Transformation* (1. p., ss. 119–131). Routledge. https://doi.org/10.4324/9780429490187-10

Wedenborg, F. (2015). *Toimittajan salausopas*. Mediapooli/Waasa Graphics Oy.

LIITTEET

LIITE 1

PUOLISTRUKTUROITU TEEMAHAASTATTELU
PÄÄKYSYMYSTEN RUNKO

PERUSTIEDOT
Henkilötiedot, koulutus, työkokemus, työtehtävä nyt

YLEISET KOKEMUKSET TIETOTURVASTA TOIMITUSTYÖSSÄ
- Mitä tietoturva mielestäsi tarkoittaa toimittajalle?
- Millaisia ovat omat kokemuksesi tietoturvasta työssäsi?
- Millaisena koet tietoturvaosaamisesi verrattuna kollegoihisi?
- Millaisena näet työnantajan merkityksen tietoturvallisessa työskentelyssä?
- Oletko saanut koulutusta tai opastusta tietoturva-asioihin?

KYBERTURVALLISUUSUHKIEN YMMÄRTÄMINEN JA RISKITEKIJÄT TOIMITUSTYÖSSÄ
- Miten käsität termin kyberuhka ja tietoturvauhka?
- Millaisia kyberuhkia toimittaja voi mielestäsi työssään kohdata?
- Oletko itse kokenut kyberuhkia, jos olet, millaisia ja missä tilanteessa?
- Oletko varautunut tietoturvallisuutta koskeviin uhkiin ja jos, niin miten?
- Miten koet työantajana roolin tietoturvallisessa työssä, luotatko organisaatiosi tietoturvaan ja osaamiseen?

TEKNOLOGIA JA TYÖVÄLINEET
- Millaisia on oma kokemuksesi tietoturvateknologiasta, kuten ohjelmistoista ja välineistä?
- Millaisia työvälineitä käytät toimitustyössäsi, miten niiden tietoturvasta huolehditaan?
- Millaisella tasolla työvälineidesi tietoturva mielestäsi on? Voisiko jotain tehdä toisin, mitä?
- Käytätkö omia laitteita tai ohjelmistoja työtehtävissä, jos, miksi?

LISÄKSI
+ Apukysymykset (kuvaile, kerro lisää, miten päädyit tähän tulokseen, perustele miksi päädyit tuohon johtopäätökseen)
+ Vapaa sana