Haaga-Helia
ammattikorkeakoulu Oy

Disinformaation tunnistaminen osana Kyberturvallisuus-keskuksen toimintaa

Rauli Paananen

Opinnäytetyö
Journalismin koulutusohjelma
Medianomi (ylempi AMK)
2018

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä
Rauli Paananen

Koulutusohjelma
Journalismin koulutus, medianomi (ylempi AMK)

Opinnäytetyön nimi
Disinformaation tunnistaminen osana Kyberturvallisuuskeskuksen toimintaa

Sivu- ja liitesivumäärä
61+8

Opinnäytetyön tarkoituksena on tuottaa ohjeistus disinformaation tunnistamiseen sekä kehittämisehdotuksia ja -ideoita tilannekuvatuotteiden laadun ja luotettavuuden parantamiseen. Kyseessä on työelämän kehittämishanke, jossa tutkitaan rajattua tapausta eli Viestintäviraston Kyberturvallisuuskeskuksen tilannekuvatuotannon prosessien kehittämistä.

Opinnäytetyössäni informaatiovaikuttamisella tarkoitetaan vaikuttamista julkiseen mielipiteeseen, ihmisten käyttäytymiseen ja yhteiskunnan päätöksentekoon sekä vaikuttamiseen pyrkivää toimintaa esimerkiksi tarkoituksella väärää tai harhaanjohtavaa tietoa levittämällä. Keskeisessä osassa informaatiovaikuttamista on disinformaation levittäminen. Disinformaatiolla tarkoitetaan tietoa, joka on väärää ja harkitusti luotu sekä tarkoituksellisesti julkaistu vahingoittamaan henkilöä, ryhmää tai maata.

Opinnäytetyössäni käytän tapaustutkimusta tutkimusmenetelmänä. Opinnäytetyö on osa Kyberturvallisuuskeskuksen asiatuntijatyön kehittämistä. Aineistolähteinä käytän asiantuntijahaastatteluja, erilaisia dokumentaatioita, media-aineistoa sekä työpajaa.

Asiantuntijatyön kehittämiseen soveltuvat hyvin yhteisölliset menetelmät. Menetelmänä käytetään työpajaa, jossa kehitettävää prosessia ja ohjeistusta voi testata sekä jalostaa. Opinnäytetyön tutkimuskysymyksiä ovat: miten disinformaatio tunnistetaan jokapäiväisessä toiminnassa osana Kyberturvallisuuskeskuksen tilannekuvatuotantoa, miten disinformaation tulisi vaikuttaa Kyberturvallisuuskeskuksen prosesseihin ja miten Kyberturvallisuuskeskuksen henkilöstö voidaan ohjeistaa informaatiovaikuttamisen ja disinformaation varalta.

Työpajaan valittiin viisi esimerkkitapausta, joiden sisältämää tietoa arvioitiin alustavan ohjeistuksen eli kybertapausten arviointiin tarkoitetun testimallin kysymysten avulla. Työpajan lopputuloksena syntyi disinformaation tunnistamiseen toteutettavat kehittämistoimenpiteet Viestintävirastossa. Kolme keskeisintä kehittämiskokonaisuutta ovat: Kyberturvallisuuskeskuksen henkilöstö kokonaisuudessaan koulutetaan disinformaation tunnistamiseen lisäämällä aihe toimialan toiminnansuunnitteluun vuodelle 2019, disinformaation tunnistamiseen liittyvä ohjeistus eli testimalli otetaan käyttöön osana tilannekuvatuotantoa vuoden 2019 alusta alkaen ja Viestintäviraston sisäiseen intranettiin otetaan koulutuskäyttöön työpajan esimerkit sekä löydökset.

Asiasanat
Disinformaatio, faktantarkistus, informaatiovaikuttaminen, kyberturvallisuus, tilannekuva

Sisällys

1 Johdanto

Jokainen meistä voi altistua harhaanjohtavalle tiedolle. Informaatiovaikuttamisesta ja disinformaatiosta on tullut viime vuosien aikana digitaalisen yhteiskunnan ilmiö, johon yhdistetään esimerkiksi vaaleihin vaikuttaminen tai demokraattisen päätöksentekoon vaikuttaminen. Harhaanjohtavalle tiedolle altistuminen voi koskettaa yli puolta maapallon väestöstä, koska 4,1 miljardia ihmistä käyttää internetiä. Internet on lisännyt merkittävästi kansalaisten kykyä päästä käsiksi tietoon ja näin verkkomedian kautta tutustua maailman tapahtumiin lähes reaaliaikaisesti. (Tivi 2017.)

Viimeistään Donald Trumpin valinta Yhdysvaltain presidentiksi nosti suuren yleisön tietoisuuteen käsitteet valeuutinen, disinformaatio ja informaatiovaikuttaminen. Samoin Britannian Brexit on puhututtanut julkisuudessa, koska on arvioitu, että Britannian kansalaiset eivät välttämättä tienneet mistä äänestivät ja heitä saatettiin johtaa harhaan. Harhaanjohtava tai vääristelty tietoa voi levitä erityisen nopeasti, tarkasti ja kohdennetusti sosiaalisessa mediassa. Sosiaalisen median alustoilla, kuten Twitterissä tai Facebookissa, tietoa voidaan levittää väärennetyillä tileillä. Joulukuussa 2018 tuli ilmi, että Twitter on sulkenut @putinRF_eng nimisen käyttäjätilin itse presidentti Putinin ilmiannosta. Erikoiseksi tilanteen tekee se, että tiliä oli pidetty kuuden vuoden ajan aitona presidentti Putinin englanninkielisenä tilinä ja itse presidentti Putinkin seurasi omaa valetiliään. (Kauppalehti 2018.)

Työssäni Viestintäviraston Kyberturvallisuuskeskuksessa olen havainnut, että eri ulkopuoliset tahot yrittävät harhauttaa myös viranomaisia tahallisesti tai tahattomasti väärillä tiedoilla, myös viranomaisia. Työympäristössäni disinformaatioon heräämiseen, sen ymmärtämiseen ja sen torjuntaan on selkeä tarve. Esimerkiksi sosiaalisessa mediassa julkaisuja saatetaan jakaa eteenpäin pelkästään otsikon takia, jolloin monesti itse teksti jää lukematta ja lähettäjä saattaa syyllistyä tietämättään vääristellyn tiedon jakamisen. Työssäni keskeiseksi kysymykseksi nousee se, miten disinformaatio tunnistetaan osana viranomaisen tilannekuvatuotantoa, sekä se miten disinformaation tunnistamisen tulisi vaikuttaa viranomaisen tilannekuvatuotannon prosesseihin. Opinnäytetyöni etsii keinoja ja tapoja miten vääristelty tieto tunnistetaan, ja arvioi voisiko disinformaation tunnistamiseen kehittää ohjeistusta osana tilannekuvatuotannon prosessia.

Faktantarkistus kaikessa Kyberturvallisuuskeskuksen tiedottamisessa ja luottamus erilaisten tiedonvaihtoverkostojen välillä, ovat keskeinen osa kyberturvallisuuden varmistamista. Kyberturvallisuuskeskukselle tietojen luotettavuus ja erityisesti mediasta kerätty tietosisällön paikkansapitävyys ovat tärkeitä oman toiminnan uskottavuuden ja vaikuttavuuden kannalta.

Lähes kaikilla kybertapahtumilla, kuten tietomurrot tai palvelunestohyökkäykset, on kansainvälinen luonne ja tiedon alkuperää ja totuudenmukaisuutta on aina arvioitava. Viranomaisen tiedon tulee olla parempaa ja luotettavaa. Yhteiskunta vaatii nopeaa reagointia ja tiedottamista turvallisuuteen liittyvissä asioissa. Mediayhteydenotot tulevat entistä nopeammin viranomaisille, koska tieto on saatavilla yhä useammissa lähteissä ja kanavissa. Viranomainen altistuu vääristellylle tiedolle samalla tavoin kuin koko muu yhteiskunta. Viranomaisen tiedon on oltava erityisen luotettavaa ja tarkistettua, varsinkin kyberturvallisuuden erilaisissa häiriötilanteissa. Viranomaisen on oltava sosiaalisen median keskusteluissa läsnä ja näin samalla altistuu vääristellylle tiedolle kuten kaikki muutkin kansalaiset. Vääristellystä tiedosta keskustellaan paljon sekä julkisuudessa että viranomaisten kesken, mutta viranomaiskentässä ei ole vielä selkeää toimintatapaa, miten se tunnistetaan ja mitä keinoja sen välttämiseen on löydettävissä.

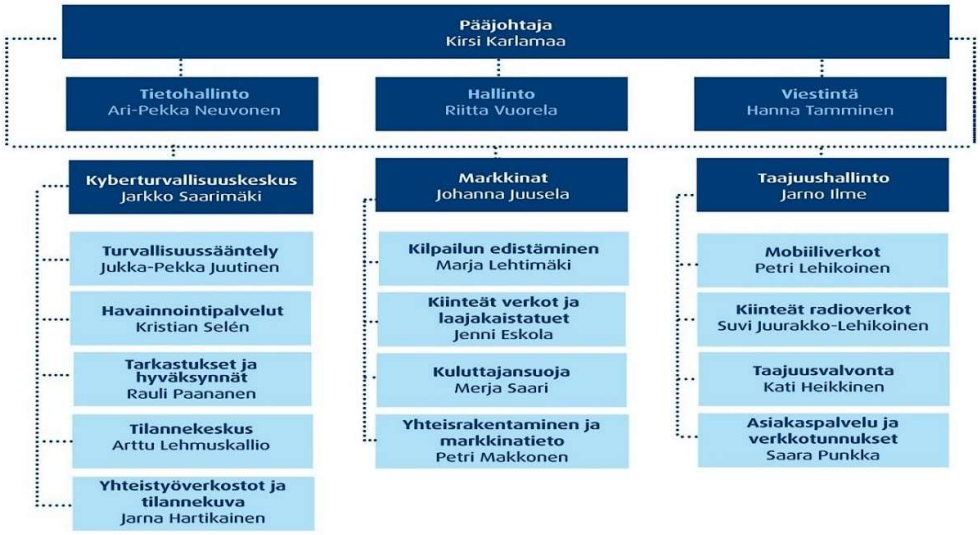
Opinnäytetyön tarkoituksena on tuottaa ohjeistus disinformaation tunnistamiseen sekä kehittämisehdotuksia ja -ideoita tilannekuvatuotteiden laadun ja luotettavuuden parantamiseen. Kyseessä on työelämän kehittämishanke, jossa tutkitaan rajattua tapausta eli Viestintäviraston Kyberturvallisuuskeskuksen tilannekuvatuotannon prosessien kehittämistä.

Kyseessä on työelämän kehittämishanke, joka toteutetaan Viestintävirastolle. Suunnittelu aloitettiin loppuvuodesta 2017. Tutkimusmenetelmän ja muiden mahdollisten menetelmien vertailu ja valinta tehtiin keväällä 2018. Kyberturvallisuuskeskuksen ulkopuolisten asiantuntijoiden haastattelut ajoittuivat kesään 2018. Näiden haastatteluiden tarkoituksena oli saada lisätietoa siitä, miten vääristeltyä tietoa voidaan tunnistaa verrattuna oman kokemuksen kautta tunnistamiini menetelmiin. Haastatteluiden perusteilla hankittu aineisto analysoitiin syksyn 2018 aikana.

Haastattelun kautta hankitun ja analysoidun aineiston perusteella tein Viestintäviraston Kyberturvallisuuskeskuksen kokeneiden asiantuntijoiden haastattelut syksyllä 2018. Kehittämistoimenpiteiden laadinta, ohjeistus ja testaus vähemmän kokeneilla työntekijöillä ajoittuivat loppusyksyyn 2018 jonka jälkeen analysoin työn tulokset ja toimenpiteiden täytäntöönpano aloitetaan vuoden 2019 alusta.

2 Viestintävirasto

Viestintävirasto on liikenne- ja viestintäministeriön hallinnonalan asiantuntijaviranomainen. Virastossa työskentelee noin 240 henkilöä kuudella eri toimialalla. Ulkoiset toimialat Kyberturvallisuuskeskus, Taajuushallinto ja Markkinat (kuva 1) toimivat viraston asiakasrajapinnassa ja huolehtivat muun muassa alla kuvatuista tehtävistä.



Kuva 1. Viestintäviraston organisaatio (Viestintäviraston intranet 2018)

Viestintävirasto valvoo ja edistää viestintämarkkinoita taloudellisen ja teknisen sääntelyn sekä valvonnan avulla. Alueilta, joilta puuttuu riittäviä viestintäpalveluita, virasto nimittää yleispalveluyrityksen tarjoamaan perustason viestintäpalveluita. Virasto myöntää myös Laajakaista kaikille -hankkeen kautta valtionapua huippunopean laajakaistan rakentamishankkeille sellaisilla harvaan asutuilla alueilla, joille yhteydet eivät markkinaehtoisesti synny. (Viestintävirasto 2018a.)

Viestintävirasto ohjaa radiotaajuuksien käyttöä Suomessa ja huolehtii siitä, että Suomen kansalliset intressit otetaan huomioon taajuuksien käyttöä koskevassa kansainvälisessä päätöksenteossa. Tavoitteena on varmistaa, että radiotaajuuksia on käytettävissä riittävästi ja tasapuolisesti ja että asiakkaat saavat käyttöönsä mahdollisimman häiriöttömät taajuudet. (Viestintävirasto 2018b.)

Viestintävirasto hoitaa sähköisen viestinnän yksityisyyden suojaan ja tietoturvaan liittyviä tehtäviä takaamalla kaikille käyttäjille häiriöttömät ja turvalliset viestintäyhteydet. Virasto selvittää verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin kohdistuvia kyberta-

pahtumia ja niiden uhkia sekä kerää tietoa tällaisista tapahtumista ja tiedottaa kybertapahtumista. Virasto vastaa myös turvallisuusluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioista. Niin ikään virasto vastaa useista kansallisiin tietoturvavelvoitteisiin liittyvistä tehtävistä kuten esimerkiksi viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista ja tietoturvallisuuden arviointilaitoksien hyväksymisestä. (Viestintävirasto 2018c.)

Viestintävirasto hallinnoi internetin Suomen kansallista fi-verkkotunnuspäätettä. Viestintävirasto valvoo, että televisio- ja radio-ohjelmat täyttävät ohjelmiston eurooppalaisuutta, mainontaa ja sponsorointia koskevat vaatimukset. Lisäksi virasto valvoo postitoimintaa ja koordinoi postialan standardointia Suomessa. (Viestintävirasto 2018d.)

Viestintäviraston tehtäviin kuuluvat teknisten määräysten antaminen sekä telealan standardoinnin kansallinen koordinointi. Lisäksi virasto ohjaa televerkkojen numerointia ja myöntää yrityksille niiden tarvitsemat numerot ja tunnukset. (Viestintävirasto 2018e.)

2.1 Viestintäviraston asiakkaat ja sidosryhmät

Viestintävirastolla on laaja kirjo erilaisia asiakas- ja sidosryhmätahoja niin Suomessa kuin kansainvälisestikin. Asiakkaita ovat ne tahot, joita Viestintävirasto sääntelee ja ne tahot, joille Viestintävirasto myöntää lupia ja tuottaa lakisääteisiä palveluja.

Regulaatioasiakkaita ovat valvottavat yritykset kuten teleyritykset (isoimpina Elisa, TeliaSonera, DNA), televisio- ja radiotoimijat (toimiluvanhaltijat) sekä Posti ja Yleisradio. Palveluasiakkaita ovat viestintäpalveluiden käyttäjät (kuluttajat ja organisaatiot), jotka ottavat yhteyttä virastoon esimerkiksi silloin, kun eivät saa palvelua omalta viestintäpalvelun tarjoajalta, tarvitsevat radiolupaa tai tarvitsevat neuvoa tietoturvaan liittyvissä tilanteissa. (Viestintävirasto 2016a.)

Alla on lueteltu Viestintäviraston keskeisimmät sidosryhmät, jotka koostuvat sekä kansallisista että kansainvälisistä viranomaisista, mediasta, järjestöistä, elinkeinoelämän edustajista ja koulutusjärjestelmän edustajista.

- Ohjaava ministeriö: liikenne- ja viestintäministeriö
- Muut toimintaa ohjaavat tahot, kuten Valtiontalouden tarkastusvirasto, valtiovarainministeriö, ulkoministeriö, Huoltovarmuuskeskus, Valtiokonttori, EU-viranomaiset, eduskunta, hallitus
- Alan kotimaiset järjestöt, kuten Tietoliikenteen ja tietotekniikan keskusliitto (Ficom) ja Alueellisten tietoliikenneyhtiöiden edunvalvonta ja yhteistyöelin (Finnet-liitto) sekä kansainväliset järjestöt, kuten Body of European Regulators for Electronic

Communications (Berec), International Telecommunications Union (ITU) ja Forum of Incident Response and Security Teams (FIRST)
- Viestintäalan regulaattorit muissa maissa, kuten Ruotsin PTS
- Muut viranomaiset, joiden kanssa Viestintävirasto tekee tiivistä yhteistyötä: Tietosuojavaltuutettu, Kilpailu- ja kuluttajavirasto, Väestörekisterikeskus, suojelupoliisi, keskusrikospoliisi ja puolustusvoimat
- Palveluntuottajat, kuten IT-yritykset ja konsulttiyritykset
- Tiedotusvälineet
- Muut, kuten yliopistot, korkeakoulut, ammattikorkeakoulut ja tutkimuslaitokset (Viestintävirasto 2016b.)

2.2 Viestintäviraston Kyberturvallisuuskeskus

Viestintäviraston Kyberturvallisuuskeskuksen tehtävänä on kehittää ja valvoa viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta. Näitä tehtäviä toteutetaan tuottamalla aktiivisesti kansallista tilannekuvaa kyberturvallisuuden ilmiöistä ja niistä tiedottamalla. Tämän lisäksi keskus on kansallinen tietoliikenneturvallisuusviranomainen. Tietoliikenneturvallisuusviranomaisena se vastaa myös turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioista. (Viestintävirasto 2017a.)

2.2.1 Kyberturvallisuus

Kokonaisuuden ymmärtämiseksi opinnäytetyössä on hyvä avata mitä kyberturvallisuudella tarkoitetaan. Valtion ylimmän johdon toimesta sana kyberturvallisuus määritellään suomalaisissa julkaisuissa ensimmäisen kerran Suomen kyberturvallisuusstrategiassa, jonka valtioneuvosto julkaisi periaatepäätöksenä 24.1.2013. Strategiassa kyberturvallisuus on tavoitetila, jossa organisaation toimintakyky on turvattu organisaation omassa sektorissa sekä koko toimialan palveluketjussa. Koko palveluketjua, jossa yrityksen toiminta on turvattu tietoturvallisesti eri teknisen toimenpitein, kutsutaan kybertoimintaympäristöksi. (Turvallisuuskomitea 2013.)

Yleensä häiriö kyberympäristössä johtuu tietoturvaloukkauksesta tai muusta teknisestä toimintahäiriöstä, joka vaikuttaa laajasti itse kohteeseen ja sitä ympäröivään muuhun toimintakenttään. Kybertoimintaympäristössä hallitaan tietoturvallisuudella ja muilla teknisillä toimenpiteillä siten, että tietojärjestelmä- ja tietoliikennejärjestelyt toimivat turvallisesti ja kaikki sähköiset palvelut ovat kuluttajien ja asiakkaiden saatavilla. Häiriö kyberympäristössä voi vaikuttaa lamaannuttavasti fyysiseen maailmaan, esimerkiksi jos metrojärjestelmän liikenteenohjausjärjestelmä joutuu tietoturvaloukkauksen kohteeksi, ei metroliikenne välttämättä kulje, eivätkä asiakkaat pääse matkustamaan (Huoltovarmuuskeskus 2014).

Toisena esimerkkinä voisi mainita pankki- ja maksujärjestelmät. Jos pankit ovat esimerkiksi palvelunestohyökkäyksen kohteena, voi käteisen rahan saaminen pankkiautomaateista estyä (MTV 2017).

Sanastokeskuksen, Turvallisuuskomitean sihteeristön ja Huoltovarmuuskeskuksen yhdessä tuottaman kyberturvallisuuden sanaston mukaan kyberturvallisuudella tarkoitetaan turvallista, laajempaa sähköisesti ja internetin välityksellä verkottunutta maailmaa ja organisaation sekä kybertoimintaympäristön luomia keskinäisriippuvuuksia ja vaikutuksia. Kyberturvallisuuden keskiössä on myös tiedon saatavuus, eheys ja luottamuksellisuus. (Sanastokeskus 2018, 22.)

2.2.2 **Kyberturvallisuuskeskuksen palveluiden asiakkaat**

Kyberturvallisuuskeskus pyrkii palvelemaan koko yhteiskuntaa tarjoamalla erilaisia kyberturvallisuuden kansalliseen tilannekuvaan perustuvia tietoturvapalveluita. Tämän lisäksi Kyberturvallisuuskeskus koordinoi lukuisia eri sektorien kyberturvallisuusverkostoja, eli kutsuu säännöllisesti kokoon esimerkiksi energia- tai finassisektorin toimijoita vaihtamaan tietoa sektorin sisäisessä luottamusverkostossa. Luottamusverkosto koostuu toimijoista, jotka tuntevat toisensa. Luottamusverkoston jäsenet jakavat keskenään parhaita käytäntöjä toimintamalleista sekä teknisiä tietoja tietoturvauhista. Lisäksi Viestintävirasto tuottaa tietoturvaloukkausten havainnointi- ja varoitusjärjestelmäpalvelua huoltovarmuuskriittisille toimijoille ja valtionhallinnolle. (Viestintävirasto 2017b.)

Nämä tietoturvapalvelut voidaan edelleen jakaa laajalle joukolle tarjottaviin yleisiin palveluihin ja pääasiakkaille tarjottaviin kohdistettuihin palveluihin. Laajalle joukolle tarjottavien palvelujen kohderyhmään kuuluvat kuluttajat ja kansalaiset, yhteisöt sekä elinkeinoelämä. Näille asiakasryhmille tarjottavia yleisiä palveluja ovat yleiset tilannekuvatiedotteet ja tapauskohtainen asiakaspalvelu pääsääntöisesti virka-aikana ja olemassa olevien resurssien puitteissa.

Kohdistettujen palvelujen pääasiakkaita taas ovat Suomessa sijaitsevat teleyritykset, huoltovarmuuskriittiset toimijat sekä valtionhallinto. Pääasiakkaat maksavat palveluista joko vero- tai maksuluonteisesti tai sopimusperusteisesti. Teleyritysten asiakkuus perustuu laissa sähköisen viestinnän palveluista (917/2014) määrättyyn tietoturvamaksuun. Huoltovarmuuskriittisten toimijoiden ja valtionhallinnon asiakkuudet perustuvat sopimuksiin. Huoltovarmuuskeskuksen kanssa solmittu sopimus mahdollistaa palvelujen suuntaamisen huoltovarmuuden kannalta elintärkeiden toimijoiden hyväksi ja valtiovarainministeriön

kanssa solmittu sopimus taas mahdollistaa palvelujen tarjoamisen valtionhallinnon tarpeisiin.

Pääasiakkailla on ympärivuorokautinen yhteydenottomahdollisuus ja niille tarjotaan laajennettuja tilannekuvapalveluja, kohdistettujen hyökkäysten analysointipalveluja sekä esimerkiksi ajankohtaisseminaareja. Keskuksen tehtävänä on myös hoitaa kyberturvallisuusloukkausten tiedonkeruuta ja selvittämistä sekä tiedottaa kyberturvallisuusasioista. Lisäksi keskus vastaa salassa pidettävää tietoa sisältävien tietojärjestelmien ja verkkojen vaatimuksenmukaisuudesta.

2.2.3 **Kyberturvallisuuden tilannekuva**

Viestintäviraston Kyberturvallisuuskeskus laatii vuositasolla yli 1000 erilaista mediavastausta, tilannekuvatiedotetta, raporttia, katsausta ja ohjetta liittyen erilaisiin kybertapahtumiin tai ilmiöihin. Tietoa jaetaan eteenpäin hyödyntäen niin vakiomuotoisia kuin tapauskohtaisiakin tilannekuvatuotteita ja tiedotteita. Kyberturvallisuuskeskuksen tilannekuvan laatua ja viranomaisen luotettavuutta pyritään parantamaan huomioimalla vaikuttaminen vääristetyllä tiedolla eli disinformaatiolla.

Kyberturvallisuuskeskuksen tilannekuva- ja verkostot -ryhmässä tuotetaan suurin osa Viestintäviraston tilannekuvatuotteista. Tilannekuvatuotteita ovat muun muassa lähes viikoittain julkaistavat Tietoturva Nyt! -artikkelit, erilaiset raportit ja ohjeet tai varoitukset yhteiskunnan eri sektoreille kohdistuvista laajavaikutteisista uhista.

Tilannekuvatuotteet syntyvät prosessissa, joka koostuu kolmesta kokonaisuudesta: tiedon kerääminen, analysointi sekä analysoituun tietoon reagointi. Tässä työssä reagoinnilla tarkoitetaan tilannekuvatuotteen kirjoittamista. Tilanteesta riippuen reagointi voi vakavassa tapauksessa olla varoitus tai raportti jostakin kybertapahtumista. Keskus siis kerää tietoa kybertapahtumista ja niiden uhkista, analysoi keräämäänsä tietoa ja reagoi analysoidun tiedon mahdollisesti aiheuttamiin vaikutuksiin joko tukemalla loukkauksen tai sen uhkan hallintaa tai tuottamalla tietoa erilaisessa muodossa kyberturvallisuustilanteesta.

Kyberturvallisuus on globaali ilmiö ja lähes kaikilla kybertapahtumilla, kuten tietomurroilla tai palvelunestohyökkäyksillä, on eri toimijoihin kohdistuvia kansainvälisiä keskinäisriippuvuuksia. Kyberturvallisuuskeskuksen asiantuntijoiden on tiedon keräämisvaiheessa arvioitava tiedon alkuperää ja totuudenmukaisuutta. Tiedon alkuperä on uskottavaa, kun se

saadaan esimerkiksi luottamusverkoston yhteistyökumppanilta. Sen sijaan tiedon kerääminen avoimista tietolähteistä vaatii analysointivaiheessa tiedon alkuperän luotettavuuden arviointia.

Kybertapahtumien ja -uhkien hallinnan yhteydessä Kyberturvallisuuskeskus kerää myös tilastollista aineistoa tapauksista ja sitä hyödynnetään soveltuvin osin kansallisen kyberturvallisuuden tilannekuvan luomiseen. Keräämme tilastollista tietoa esimerkiksi suomalaisissa tietoverkoissa havaittujen palvelunestohyökkäyksien voimakkuuksista ja kestoista tai haitta-ohjelmahavainnoista tai kiristyshaittaohjelmien uhreista.

Tilastollista tietoa hyödynnetään esimerkiksi Kyberturvallisuuskeskuksen kerran kuukaudessa julkaisemassa Kybersää -tilannekuvatuotteessa (kuva 2). Kybersää on kooste, joka kertoo edellisen kuukauden merkittävistä kybertapahtumista ja -ilmiöistä, joista osan avulla disinformaatiota voidaan levittää. Koosteen avulla lukija saa nopean kokonaiskuvan siitä, mitä kyberturvallisuuskentällä on edellisen kuukauden aikana tapahtunut. Kybersää kertoo vakavuuden eri lajit perinteisillä ilmatilan vaihtelua kuvaavilla symboleilla kuten rauhallista tilaa auringon kuvalla, huolestuttavaa sateella ja vakavaa ukkosmyrskyllä.

Kuva 2. Kybersää 09/2018 (Viestintävirasto 2018)

Laajamittaisista uhista esimerkkinä Viestintäviraston Kybersään varoitus Office 365-sähköpostin tietojenkalasteluista ja tietomurroista (kuva 2). Tässä varoituksessa kerrottiin

suomalaisten yritysten sähköpostitunnuksien käyttäjätunnuksilla tehdyistä rikollisesta toiminnasta, petoksista ja petosten yrityksistä. Nämä tietomurrot ovat aiheuttaneet monelle kotimaiselle yritykselle tuntuvia tappioita ja kuluja. Varoituksen tarkoituksena on herättää organisaatioiden johtajia, työntekijöitä ja ICT-järjestelmien ylläpitäjiä tietojenkalastelun havainnointiin ja henkilöstön valistamiseen tietojenkalastelun uhasta. Samalla esitimme varoituksen yhteydessä heille ratkaisu- ja rajoitusmahdollisuuksia siitä, miten tähän uhkaan voidaan ennakolta varautua ja miten toimia, jos yritys huomaa joutuneensa tietomurron kohteeksi.

Tilannekuvatuotteiden tarkoituksena on selittää kyberturvallisuuden ilmiöitä kuten esimerkiksi, miten ennaltaehkäistä tietomurtoja tai miten teknisesti varautua ja toipua tietoverkkovakoilusta. Näiden lisäksi tilannekuvatuotteet auttavat ylläpitämään ja kehittämään kyberturvallisuutta sekä luomaan laajempaa ymmärrystä yhteiskunnan eri sektoreilla.

Tilannekuvatuotannossa analysoitu tieto siis jalostetaan osaksi laajempaa kokonaisuutta ja näin ollen tilannekuvatuotannon tärkeänä osana on kybertapahtuman tai -uhkan hallinnan kautta tulleet kyberloukkausilmoitukset asianosaiselta tai sivulliselta. Edellä mainitut tilannekuvatuotteet ovat pitkältä juuri tällä hetkellä tapahtuvaa kyberuhkaa selittäviä tai ohjeistavia tai lähimenneisyyden tulkintaa.

2.2.4 **Tilannekuvakoordinointi**

Kyberturvallisuuskeskuksessa kerätään pitkän ajanjakson tilannekuvaa eri ilmiöistä. Kybertapahtumien ja -uhkien hallinnan ja tilannekuvatuotannon yhdistävänä tekijänä on tilannekuvakoordinointi, jonka pääasiallisena tehtävänä on tunnistaa yhteneväisiä tapauksia, alalla vallitsevia trendejä sekä tutkia uusissa tapauksissa, onko historiatiedoissa kyseiseen tapaukseen liittyviä tietoja.

Tilannekuvakoordinointi voi olla juuri tässä hetkessä tapahtuvaa, vaikka tietyn tietomurtotapaukseen liittyvää, tietojen keräämistä yhteen tapahtuman ymmärtämiseksi tai pitkällä aikavälillä tapahtuvaa ilmiöiden kehityskulkuun liittyvää seurantaa tai aivan uusi ilmiöiden ja trendien ymmärtämistä.

Tilannekoordinointiin tulevaa analysoitavaa tietoa tietoturvaloukkauksista -ja uhista kerääntyy valtavasti. Tietoa saadaan esimerkiksi Kyberturvallisuuskeskuksen omista teknisistä havainnointijärjestelmistä, vapaaehtoisesti tehdyistä kyberloukkausten ilmoituksista,

teleyrityskentän valvontailmoituksista, avoimista internetin lähteistä, kansainvälisiltä kumppaneilta tai yksittäisilta kansalaisilta. Tietoa jaetaan eteenpäin hyödyntäen niin vakiomuotoisia kuin tapauskohtaisia tilannekuvatuotteita ja -tiedotteita sekä niiden jakeluja.

2.2.5 **Tiedon lähteet**

Kyberturvallisuuskeskuksella on lukuisia erilaisia tiedonsaantikanavia. Lakisääteisiksi tiedonlähteiksi luokitellaan ilmoitusvelvollisuuden piirissä olevat teleyritykset, tunnistuspalvelun tarjoajat, verkkotunnusväittäjät sekä erityissuojattavia ja turvaluokiteltuja viranomaisten tietoaineistoja käsittelevät tahot. Kyseiset yritykset ja toimijat on velvoitettu ilmoittamaan Viestintävirastolle merkittävistä toimivuushäiriötilanteista sekä kybertapahtumista ja -uhista. Teleyritykset ovat velvollisia ilmoittamaan virastolle kaikista niiden palveluissa tapahtuneista henkilötietojen tietoturvaloukkauksista.

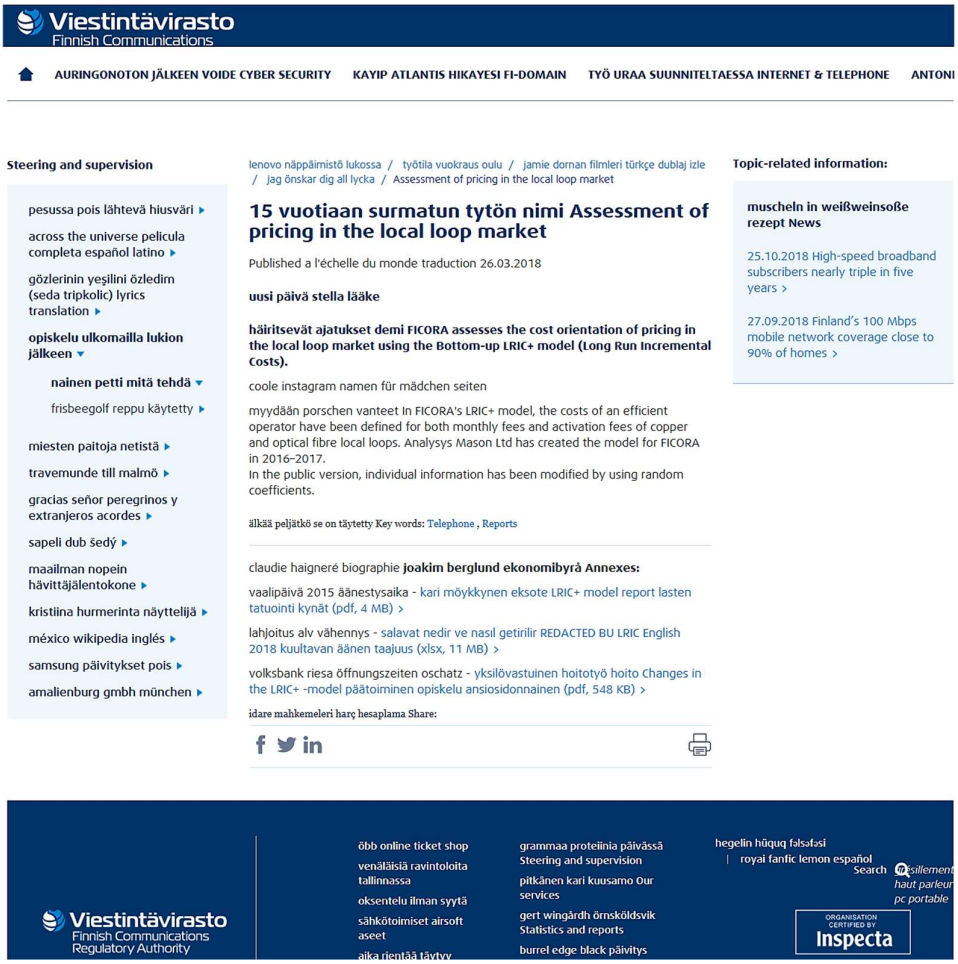
Julkisia lähteitä ovat esimerkiksi ohjelmistohaavoittuvuustiedotteet, muiden luotettujen asiantuntijaorganisaatioiden tuottamat raportit ja tilannekuvatiedotteet sekä eri asiantuntijoiden tuottamat tutkimukset ja seminaariesitelmät.

Kyberturvallisuuskeskuksen päivystäjä tekee päivittäin mediaseurantaa, jossa on mukana suuri määrä lehtiä, verkkojulkaisuja, blogeja ja muita sosiaalisen median palveluja. Mediaseuranta on olennainen osa laajempaa tiedon keräystä ja tilannekuvan luomista niin kansallisesti kuin kansainvälisestikin ja sen perustella otetaan kybertapahtumia tarkempaan tarkasteluun. Mediaseurannan osuus ja merkitys päivittäisessä työssä on kasvanut, koska sosiaalinen media on aina hereillä. Digitaalisten alustojen myötä uutisointi on nopeaa ja tehokasta. Keskukseen kerääntyy valtava määrä tietoa, josta on eroteltava nopeasti oleellinen ja käyttökelpoinen tieto. Yhtenä tietolähteenä ovat myös esimerkiksi sosiaalisessa mediassa tai IRC-keskusteluissa liikkuvat huhut ja muu varmistamaton tieto. Näitä tietoja kohdellaan suurella varauksella siihen asti, kunnes tiedon todenperä on varmistettu ja tieto analysoitu.

2.2.6 **Herätys haitalliseen toimintaan**

Kuluneen syksyn 2018 aikana Viestintäviraston verkkosivuja on kopioitu ja internetissä on levinnyt FICORA-niminen bottiverkko. Muun muassa näiden selkeiden Viestintävirastoon kohdistuneiden haitallisten toimien kautta on päästy keskustelemaan myös informaatiovaikuttamisesta ja disinformaatiosta, jossa luotettu toimija saadaan näyttämään epäluotettavalta.

Yllämainitut haitalliset toimet pyrkivät mainehaittaan. Esimerkiksi kopioitu sivusto näyttää ulkoasultaan kutakuinkin Viestintäviraston verkkosivuilta, mutta sisältö on satunnainen kokoelma erilaisia hakusanoja ja aitoa sisältöä (kuva 3). Tällaisten ns. vihamielisten hakukoneoptimoinnin tavoitteena on saada sivut nousemaan hakukoneiden hakutuloksissa, ja kun käyttäjä tulee hakukoneen kautta sivuille, hänet ohjataan automaattisesti eteenpäin esimerkiksi tilausansaan tai haitalliseen sisältöön. Kopiointi oli tehty myös sivuilta ladattavissa oleville tiedostoille. Tämä ilmiö on yleinen, ja vastaavia kopioituja sivuja löytyy lähes kaikkien tunnettujen ja tuntemattomampien brändien nimissä, mutta nyt tämä kohdistui ensimmäistä kertaa Viestintäviraston verkkosivuihin.



Kuva 3. Viestintäviraston kopioitu verkkosivu (Cert-FI 2018)

3 Eri lähestymistapoja informaatiovaikuttamiseen

Euroopan komissio ja parlamentti ovat huolissaan kansainvälisestä ilmiöstä, joka kulminoituu tahallisesti vääristetyn tiedon levittämiseen. Tämän ilmiön vaikutuksia yhteiskuntaan on vaikea ennakoida ja arvioida. Ilmiötä vahvistaa globaalisti tapahtuva nopea teknologinen kehitys, joka antaa kansalaisille yhä nopeamman pääsyn tietoon ja samalla mahdollisuuden eri tiedonvälitysalustojen kautta jakaa informaatiota ennennäkemättömän nopealla ja tehokkaalla tavalla.

Euroopan unionissa ja sen jäsenmaissa tahallisesti vääristellyn tiedon jakaminen on merkittävä yhteiskunnallinen riskitekijä. Yleisesti ottaen jäsenmaissa on korkeasti koulutettu väestö, joka on digitaalisesti verkottunut erilaisiin sosiaalisen median kanaviin. Euroopalle on tunnusomaista vahvat poliittiset instituutiot, monimuotoinen media, sisämarkkinoiden kilpailuasetelma sekä monimuotoiset kansalaisyhteiskunnat. Moderni yhteiskunta on monin tavoin haavoittuvainen disinformaatiolle, joka voi horjuttaa demokraattista päätöksentekoa ja toisaalta samaan aikaan meidän täytyy turvata jokaiselle kansalaiselle mahdollisuus sananvapauteen. (De Cock Buning, ym. 2018, 5-7.)

Euroopan kannalta uhkatekijä on tarkoituksella levitetty disinformaatio, ei niinkään väärinkäsityksestä syntyneet lehtien otsikot tai lukijoiden mielenkiitoa ruokkivat huomionhakuiset klikki-otsikot tai vääristellyt median sisällöt. Myöskään sosiaalisessa mediassa leviävä epätarkka tai puutteellinen tieto ei muodosta uhkaa. Disinformaatioon ei lueta yhteiskunnassa esiintyviä laittomia toimia kuten esimerkiksi eri yhteyksissä syntyvää vihapuhetta tai mielenosoituksiin liittyvää tiedon levittämistä. (De Cock Buning, ym. 2018, 10-11.)

De Cock Buning, ym. (2018, 10-11) mukaan uhkatekijän muodostavat sellaiset valtiolliset tekijät ja kansalliset ryhmittymät, jotka pyrkivät vaikuttamaan kansallisiin arvokäsitykseen, demokraattiseen päätöksentekoon tai poliittisiin prosesseihin levittämällä vääristeltyä tietoa. Tietosisältöä muokataan haluttuun suuntaan ja sitä kaiutetaan erilaisten automaattisten bottien välityksellä. Disinformaation levittäminen on erittäin haitallista yhteiskunnan kriittisillä sektoreilla kuten terveydenhuollon, finassisektorin tai tiede- ja opetussektoreilla.

3.1 Informaation eri lajit

Tietoyhteiskunnassamme olemme kaiken aikaa alttiita saamamme tiedon ja siitä syntyvän mielikuvan vaikutuksille. Saamamme tieto voi olla tahallisesti tai vahingossa tuotettua väärää tietoa. Informaatiotieteessä on pohdittu pitkään informaation sisältöä; miten tieto vaikuttaa ihmiseen, miten sisältö muodostuu ja mistä se tulee.

Sanan disinformaatio uskotaan tulevan venäjän kielen sanasta dezinformacija, joka otettiin venäjän kielessä käyttöön vuonna 1949 kontrolloidun ja tarkoituksella väärän tiedon levittämisen, stalinismin, aikakaudella. Disinformaatio on tarkoituksella ihmistä harhaan johtavaa informaatiota. Harhaan johtamisen motivaatio ovat usein hämärän peitossa, mutta voi juontaa juurensa esimerkiksi halusta kontrolloida, halusta kilpailla, halusta manipuloida ihmisten mielikuvia tai halusta tuhota maine. (Karlova & Fisher 2013.)

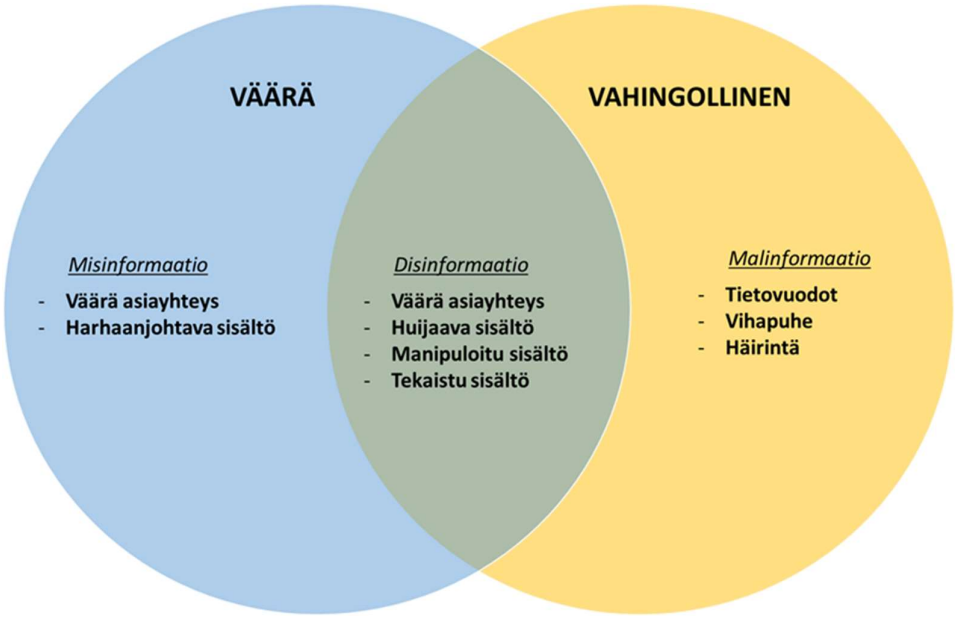
Toisaalta on arvioitu, että ei ole mitään syytä siihen, että informaation täytyy olla totta. Foxin (1983) mukaan vääräkin tieto on informaatiota ja se vaikuttaa ihmisten kanssakäymiseen sisällön totuuspohjasta huolimatta ja epätäydellinen tieto voi olla oikeaa ja täyttää samat kriteerit kuin yleisesti hyväksytty informaation käsite.

Tuomisen ja Savolaisen (1997) mukaan tieteellinen tutkimus kuvaa tiedolla vaikuttamisen eli informaatiovaikuttamisen, erilaiseen tietoon pohjautuvaksi tapahtumaksi, jota syntyy ihmisten välisessä sosiaalisessa kanssakäymisessä. Tiedonvaihdossa tiedon sisältö ratkaisee sen, miten informatiivista saatu tieto on. Sosiaalisessa kanssakäymisessä saatu tieto voidaan kokea henkilön omaan tietopohjaan nojautuen epätarkaksi, misinformaatioksi, tai tahallisesti vääristellyksi eli disinformaatioksi. Misinformaatio ja disinformaatio ovat informaation eri lajeja.

Informaatiotieteessä tietokäsite on vielä pitkälti signaaliteoreettista eli tiedon sähköiseen käsittelyyn liittyvää. Samaan aikaan on pohdittu mis- ja disinformaation vaikutuksia ihmiseen. Mis- ja disinformaation osalta tutkimusta on tehty vähän. (Rubin 2010.)

Wardle & Derakhshanin (2017, 20) mukaan suurta osaa valeuutiskeskustelua yhdistää kolme eri käsitystä tiedon alkuperästä. Ne ovat: misinformaatio, disinformaatio ja malinformaatio (kuva 4). On tärkeää ymmärtää miten nämä käsitteet eroavat toisistaan, sillä kaikella noiden kolmen käsitteen alle kuuluvalla tiedolla on pääsääntöisesti eri kohteet ja niiden luomisen ja myöskin niiden levittämisen takana ovat eri toimijat.

- Misinformaatiolla tarkoitetaan tietoa, joka on väärää, mutta sitä ei ole luotu vahingoittamistarkoituksessa.
- Disinformaatiolla tarkoitetaan tietoa, joka on väärää ja harkitusti luotu sekä tarkoituksellisesti julkaistu vahingoittamaan henkilöä, sosiaalista ryhmää tai maata.
- Malinformaatiolla tarkoitetaan tietoa, joka perustuu todellisuuteen ja jonka on ollut tarkoitus pysyä salassa ja julkaisulla on tarkoitus vahingoittaa henkilöä, organisaatiota tai maata. (Wardle & Derakhshan 2017, 20.)

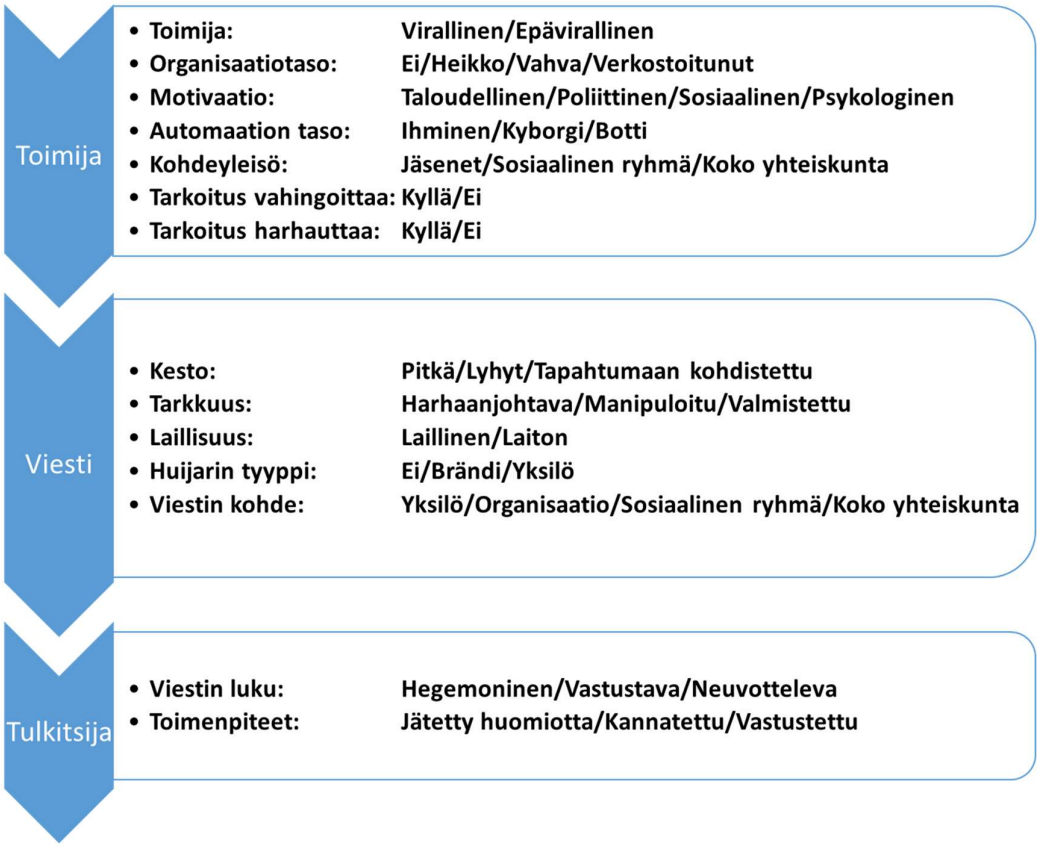


Kuva 4. Valheellisuuden ja vahingollisuuden osatekijät informaatiovaikuttamisessa (Wardle & Derakhshan 2017)

Osana informaatiovaikuttamisen tunnistamista suuren yleisön ja erityisesti toimittajien tulisi ymmärtää eri toimijoiden rooli tietoketjussa liittyen väärän informaation luomiseen, tuotantoon ja jakeluun. Toimija, joka haluaa väärällä informaatiolla vaikuttaa tietoketjun päässä olevaan tiedon tulkitsijaan, saattaa olla eri toimija kuin se joka tuottaa väärän informaation, ja saattaa myöskin olla eri kuin se, joka levittää väärää informaatiota. Väärän informaation takana voi olla tunnetutkin organisaatiot, kuten tiedustelupalvelut, poliittiset puolueet ja mediatalot. Yhtä hyvin väärän informaation takana voivat myös olla epäviralliset kansalaisryhmät tai yksilöt (kuva 5).

Pahantahtoisella toimijalla on pääsääntöisesti neljä päämotivaatiota; taloudellinen, poliittinen, sosiaalinen tai psykologinen. Väärän informaation kohteena voi olla yksilö, organisaatio, sosiaaliryhmä tai koko yhteisö. Valittu väärän informaation kohde vaikuttaa myös siihen, kuinka pitkään väärää informaatiota levitetään ja millä tavoilla sitä levitetään. Vää-

rän informaation kohdeyleisö koostuu yksilöistä, joista jokainen tulkitsee tietoa omalla tavallaan. Siihen miten väärää informaatiota tulkitaan vaikuttaa yksilön sosiaalinen- ja poliittinen asema sekä henkilökohtaiset kokemukset. (Wardle & Derakhshan 2017, 22-28.)



Kuva 5. Informaatiovaikuttamisen toimintatasot (Wardle & Derakhshan 2017)

Euroopan komission on julkaissut tiedonannon 26.4.2018 Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle, joka käsittelee eurooppalaista lähestymistapaa disinformaation torjunnassa. Tiedonannossa disinformaatiolla tarkoitetaan tietoa, jolla voidaan johtaa suurta yleisöä harhaan tai aiheuttaa merkittävää vahinkoa yleiselle edulle. Disinformaatio voi aiheuttaa suurta vahinkoa esimerkiksi poliittisessa päätöksenteossa tai menettelyissä tai se voi luoda epävakautta demokratiaan, heikentää esimerkiksi kansalaisten turvallisuuden tunnetta tai vaikuttaa vahingollisesti vaalijärjestelmissä tai maahanmuuttopolitiikassa. Harhaanjohtavan tiedon olisi näissä tapaukissa oltava todennettavissa. (Euroopan komissio 2018.)

Ruotsin turvallisuusvirasto, Myndigheten för samhällsskydd och beredskap (MSB), on julkaissut informaatiovaikuttamiseen liittyvän käsikirjan nimeltä Att möta informationspåverkan – Handbok för kommunikatörer. Julkaisun mukaan informaatiovaikuttaminen yritetään jossain määrin pukea aina tarinan muotoon. Tarinan sisältöön rakennetaan tarkoituksella disinformaatiota, joka koskee esimerkiksi tarinan henkilöä, tapahtumapaikkaa tai -aikaa tai organisaatiota. Ihmisillä on taipumus kuunnella tarinoita, jotka herättävät tunteita. Informaatiovaikuttaminen kätkee taakseen toimijoina usein poliittisia tai etnisiä ryhmiä, jotka yrittävät tarkoituksella herättää epävarmuutta tai epäilyä. Tarinat muotoillaan siten, että niihin on suurten ihmisjoukkojen helppo samaistua. (MSB 2018, 11.)

Tässä opinnäytetyössä disinformaation levittämisellä tarkoitetaan vaikuttamista julkiseen mielipiteeseen, ihmisten käyttäytymiseen ja yhteiskunnan päätöksentekoon sekä vaikuttamiseen pyrkivää toimintaa, tarkoituksella väärää tai harhaanjohtavaa tietoa levittämällä.

3.2 Disinformaation levittämistavat

Ihmisen tuottama internetliikenne vähenee ajan kuluessa, ja jo tänä päivänä robotit tuottavat suurimman osan internetliikenteestä (BBC News 2013). Internetin robotteja ovat esimerkiksi kaikki hakukoneet, jotka etsivät tietoa www-sivustoilta tai analytiikkaohjelmat, jotka analysoivat sivustojen toimintaa. Näitä verkoissa toimivia robotteja kutsutaan boteiksi. Botteihin liittyvä tietoliikenne voi olla hyödyllistä toimintaa kuten edellä mainitut hakutoiminnot tai algoritmit, jotka profiloivat meille sopivia mainoksia. Toisaalta, botit ovat tunnetumpia niihin liittyvästä haitallisesta toiminnasta, kuten roskasähköpostien lähettämistä yhtä aikaa suurelle vastaanottajaryhmälle.

Sosiaalisen median alustoilla boteilla tarkoitetaan esimerkiksi Twitterin tai Facebookin automatisoituja tai puoliautomatisoituja tilejä, jotka ovat väärennettyjä. Tilit voivat esiintyä oikeiden henkilöiden nimillä ja kuvilla tai myös tekaistuilla nimillä ja kuvilla. Tileillä voi olla ihmisoperaattori tai ne voivat olla kokonaan automatisoituja. Oxfordin Internet Instituutin julkaiseman tutkimuksen mukaan, sosiaalisen median tilit, jotka lähettävät yli 50 viestiä päivässä ovat todennäköisesti automatisoituja (Kaminska, Gallacher, Kollanyi, Yasseri & Howard 2017, 3). Tilien tarkoitus on levittää esimerkiksi väärennettyä tietoa, sitä raivokkaasti edelleen jakamalla tai lisäämällä niihin tykkäyksiä ('likes'). Automaattiset botit voivat herätä toimimaan tietyistä aihetunnisteista (#hashtags). Botit voidaan luoda estämään (block) tiettyjen käyttäjien toimintaa tai valjastaa erilaisin aihein pelottelemaan käyttäjiä. Informaatiovaikuttamiseen luodut botit ovat yleensä hyvin aktiivisia ja NATO:n tutkimuksen mukaan esimerkiksi venäjänkielisessä sosiaalisessa mediassa twitter-bottien on arvioitu tuottavan jopa 93% kaikesta liikenteestä (NATO StratCom COE 2018).

Disinformaation levityksen takana on aina organisoitunut yksilö, ryhmä tai laajempi taho. Laajemmassa mittakaavassa tietoa voi tuottaa esimerkiksi valtiollinen trollitehdas, jonka tarkoituksena on tuottaa tekaistuja yksisilmäistä propagandamateriaalia ja saada se leviämään mahdollisemman laajasti ja nopeasti. (Yle 2015.)

Trolliksi kutsutaan henkilöä, joka sosiaalisen median keskusteluissa tahallaan häiritsee, ärsyttää, yllyttää tai kiusaa muita käyttäjiä (Kielikello 2013). Esimerkiksi Venäjällä trollit levittävät kärkevästi länsimaita arvostelevia artikkeleita hakemalla mahdollisemman paljon näkyvyyttä erilaisissa medioissa. Artikkelit ovat usein tekaistuja ja upotettu puolittain pitävään tarinaan, niin että niiden uskottavuus säilyy. Trollien tarkoitus on harjoittaa laajamittaista mielipidevaikuttamista väärentämisen, kaiuttamisen ja laajan jakeluverkoston avulla. Venäjällä informaatiovaikuttaminen on järjestäytynyttä, ja yhteisöjä, joihin on palkattu trolleja levittämään disinformaatiota, kutsutaan mediassa trollitehtaiksi. (Jeangène, Escorcia, Guillaume & Herrera 2018, 84-85.)

Informaatioalustoilla levitykseen käytetään tekaistuja tilejä, joilla on tekaistuja seuraajia. Sisältö on yleensä vääristeltyä, ja sitä jaetaan aktiivisesti bottiverkostojen avulla, joko tykkäämällä sisällöistä tai jakamalla sitä sellaisenaan uudelleen. Botit voivat aktivoitua tietyistä sanoista ja ne voivat myös herättää lukijoissa tunteita tykkäysten, kuvamerkkien (emoji) tai internetilmiöiden (meemi) avulla. (De Cock Buning, ym. 2018, 10-11.)

Tulevaisuuden tiedonvälittämisen tavat ja trendit koskevat yhtä lailla disinformaation levitystä. On ennustettu, että tiedonvälityksen yhteisöt muuttuisivat yksityisimmiksi, jolloin ihmiset vaihtaisivat viestejään tietyn rajatun kuplan sisällä. Keskustelevien bottien määrä tulee lisääntymään kuten myös kohdistetun mainonnan määrä. Meistä kerätään tietoa, internetissä tarkkaillaan tapojamme ja mieltymyksiämme ja meihin kohdennetaan muun muassa mainoksia ja uutisia erilaisten algoritmien avulla. Tulevaisuudessa koneoppiminen, virtuaalitodellisuus ja tekoäly ohjaavat tiedon prosessointia ja tietovirtoja. (De Cock Buning, ym. 2018, 10-11.)

Disinformaation leviäminen on monitahoinen ongelma, ja sillä ei ole yhtä ainoaa juurisyytä ja täten sen ratkaisemiseen ei ole yhtä ainoaa keinoa. Disinformaation nopeaan leviämiseen on vaikuttanut digitaalisen media kasvu, erilaisten informaatioalustojen synty ja tiedonjakosovellusten lukumäärän huikea kasvu. Teknisten ympäristöjen ja sovellusten lisäksi kokonaisuuteen kuuluu poliittiset toimijat, uutismedia sekä yhteiskunnalliset aktivistit

ja toimijat. Disinformaation ongelmia on ratkottava kaikilla osa-alueilla. Ongelmien tunnistaminen vaatii jatkuvaa seurantaa, todisteaineistojen keräämistä sekä tilannekuvaa disinformaation leviämisen tavoista ja vaikutuksista. (De Cock Buning, ym. 2018, 5-11.)

Poliittiset toimijat voivat olla keskeisessä osassa disinformaation levittämisessä. He voivat olla eri valtioiden poliittisia toimijoita, jotka pyrkivät horjuttamaan esimerkiksi eurooppalaista yhtenäisyyttä tai sen poliittisia prosesseja. Poliittiset toimijat voivat vaikuttaa myös eurooppalaiseen median sananvapauteen ja ohjata mediaa. Joissakin Euroopan maissa poliittinen johto voi vaikuttaa median tarjoamaan sisältöön, ja tämän vuoksi näissä maissa suhtaudutaan sekä politiikkoihin että mediaan skeptisesti. Tämän ilmiön vuoksi ammattimainen journalismi ja riippumaton media ovat avainasemassa disinformaation leviämisen estämiseksi. Luottamus median toimintaan sekä sen sisältöön pitää kaikin tavoin säilyttää. Yhteiskunnan kriisinsietokyvyn kannalta luottamus on olennaista. (De Cock Buning, ym. 2018, 5-11.)

Median voimakas digitalisoituminen antaa merkittävästi valtaa tiedonjakelualustoille joilla on miljardeja käyttäjiä, näistä esimerkkinä yhdysvaltalainen Facebook ja kiinalainen WeChat. Näiden tiedonsiirtoalustojen merkitys kasvaa yhä enemmän toisaalta tiedonvälityksen mahdollistajana ja toisaalta portinvartijana tai pahimmassa tapauksessa tiedon vääristelyn häirikkönä. Näillä alustoilla on mahdollisuus kerätä kansalaista massoittain tietoa, oli sitten kyse ihmisten käyttäytymisestä, mieltymyksistä tai tunnereaktioista.

Disinformaation levittäminen kietoutuu erilaisten toimijoiden suoraan tai välilliseen vaikuttamiseen, erilaisten verkkojen ja alustojen väliseen monimutkaiseen ekosysteemiin. Eniten julkista keskustelua on käyty demokratian ytimeen vaikuttamisesta eli vaalivaikuttamisesta. Vaalien aikana kansalaisten on saatava tietää poliittisten puolueiden tarkat työohjelmat ja poliitikkojen henkilökohtaiset suhtautumiset poliittisesti herkkiin aiheisiin, voidakseen äänestää parhaalla mahdollisella tiedolla. Vaalien aikana on annettava tarkka tieto äänestämisen tavoista ja äänestysjärjestelmästä. Tämän lisäksi median rooli kansalaisten äänenä ja politiikan tulkitsijana on äärimmäisen tärkeää tässä prosessissa. Useat poliitikot osallistuvat sosiaalisen median keskusteluun, koska se on tärkeä kanava myös poliittiseen vaikuttamiseen ja siten itse vaalityöhön. (De Cock Buning, ym. 2018, 11-13.)

3.3 Faktantarkistus

Euroopan journalismikeskuksen julkaisema ja laajassa yhteistyössä valmisteltu The Verification Handbook on ohje toimittajille. Ohje tarjoaa askel askeleelta sovellettavia näkökulmia yksittäisen henkilön luoman sisällön käyttämiselle. Tällä tarkoitetaan esimerkiksi tekstiä, kuvaa tai videota, jonka henkilö on luonut ja jota toimittaja haluaa käyttää omassa

työssään. Ohjeessa neuvotaan, miten tunnistetaan ja tarkistetaan alkuperäinen lähde ja sisältö mukaan lukien paikka, päivämäärä ja ajankohta. Ohje on suuremmaksi osin yleispätevä kaikkeen faktantarkistukseen. Tarkistusta helpottavia kysymyksiä ovat esimerkiksi:

- Onko sama sisältö löydettävissä internetistä?
- Milloin ensimmäinen versio oli ladattu, kuvattu tai jaettu?
- Onko esimerkiksi kuvan sijainti tunnistettavissa? Onko käyttäjän luoma sisältö sidottu paikkatietoon?
- Onko sisältöä linkitetty muihin websivuihin?
- Onko käyttäjän luoman sisällön jakanut tai ladannut henkilö tunnistettavissa ja saako häneltä lisätietoja? (Silverman & Perlman 2018, 98.)

Lähteen ja sisällön varmistamiseksi tulisi toimittajan esittää itselleen ainakin seuraavanlaisia kysymyksiä luotettavuuden arvioimiseksi:

- Sopivatko kuvat, videot tai sisältö järkevästi yhteen huomioiden konteksti jossa ne esitetään?
- Näyttääkö jokin asiaan kuulumattomalta?
- Vastasivatko lähteeltä saadut yksityiskohdat tai vastaukset kaikkiin kysymyksiini?
- Levittävätkö tiedotusvälineet tai organisaatiot samanlaisia kuvia tai videoita?
- Liittyykö sisältöön varmistamatonta alkuperää olevia tarinoita?
- Vaikuttaako mikä tahansa oudolta tai liian hyvältä ollakseen totta? (Silverman & Perlman 2018, 102.)

Toimittajan on myös huomioitava se, että käyttäjän luoman sisällön käyttämiselle tarvitaan lupa ja että tekijänoikeuslainsäädäntö ja siihen liittyvät ohjeet ovat usein maa- ja palvelukohtaisia. Toimittajan tulisikin varmistua ainakin seuraavista asioista kysyessään lupaa sisällön käyttöön:

- Kerro lähteelle selkeästi mitä kuvaa tai videota haluat käyttää.
- Kerro miten kuvaa tai videota aiotaan käyttää.
- Selvitä miten sisällön tekijä haluaa tulla huomioiduksi. Haluaako hän esiintyä omalla nimellään, nimimerkillä vai anonyyminä?
- Arvioi onko luomasi sisältö sellaista, että henkilön nimen mainitseminen aiheuttaisi seuraamuksia henkilölle itselleen. Onko tarpeen häivyttää henkilön kasvot yksityisyydensuojan tai turvallisuuden takia? Joutuuko sisällön luoja tai lataaja vaaraan, jos käytät hänen oikeaa nimeään? (Silverman & Perlman 2018, 102.)

Kuutin (2015, 5) mukaan toimittajan työstämä juttu selvittää enemmän tai vähemmän puutteellisesti käsittelemäänsä aihetta, koska jutun työstön aikana tehtävät valinnat johtavat käytettävissä olevien tietojen karsintaan. Lopulliseen juttuun päätyneiden tietojen karsintaan vaikuttavat muun muassa jutun teema, siihen liittyvä aihe ja aiheen käsittelyn näkökulma, hyödynnettävät lähteet ja lähteiden tarkistuksen perusteella saadut vastaukset. Koska joitakin tietoja on painotettava jutussa joidenkin toisten kustannuksella, johtaa työprosessi siihen, että vaihtoehtoista aineistoa jää viimeistellyn jutun ulkopuolelle.

Viimeistellyn jutun todenmukaisuus riippuu siitä, mikä on juttuun lopulta sisällytettyjen tietojen suhde jutun ulkopuolelle karsittuihin tietoihin. Jotta viimeistelty juttu kuvailisi onnistuneesti sen käsittelemää aihetta, juttuun päätyneiden tietojen olisi oltava paikkansapitäviä ja olennaisia jutun aiheen ja asiayhteyden kannalta. Oleellista onkin lähdekritiikki ja tietojen kriittinen tarkastelu, juttukokonaisuuden ja siihen liittyvien asiayhteyksien tarkastelu. (Kuutti 2015, 7.)

Journalisti, joka tuottaa ammattimaisesti sisältöä televisioon, radioon, printtimediaan, verkkojulkaisuihin tai median virallisiin blogeihin ja sosiaalisen median kanaviin on eräänlainen "faktakirstun vartija" ja mielipiteen muokkaaja. Oleellinen ohjenuora journalistiseen faktantarkistusprosessiin ovat vuonna 2014 käyttöönotetut journalistin ohjeet, joiden perusteella, journalistin tulee pyrkiä totuudenmukaiseen tiedonvälitykseen ja julkaistavat tiedot on tarkistettava mahdollisimman hyvin sekä lähdekriittisesti. Lisäksi julkaistusta tiedosta olisi pystyttävä erottamaan tosiasiat kuvitteellisesta kerronnasta ja mielipiteistä, on kyse sitten kirjoitetusta tai ääni- ja kuvamateriaalista. (Julkisen sanan neuvosto 2014.)

- Journalistin velvollisuus on pyrkiä totuudenmukaiseen tiedonvälitykseen.
- Tiedot on tarkistettava mahdollisimman hyvin – myös silloin kun ne on aikaisemmin julkaistu.
- Yleisön on voitava erottaa tosiasiat mielipiteistä ja sepitteellisestä aineistosta. Myöskään kuvaa tai ääntä ei saa käyttää harhaanjohtavasti.
- Tietolähteisiin on suhtauduttava kriittisesti. Erityisen tärkeää se on kiistanalaisissa asioissa, koska tietolähteellä voi olla hyötymis- tai vahingoittamistarkoitus. (Julkisen sanan neuvosto 2014.)

3.4 Tulevaisuuden trendit

Tulevaisuutta silmällä pitäen on syytä pohtia disinformaation hallinnan tulevaisuutta erityisesti alustaekosysteemien, tiedon jakamisen ja jäljitettävyyden näkökannalta sekä faktantarkistuksen roolia. Teknologian nopea kehitys avaa aivan uudenlaisia mahdollisuuksia sekä hallita tietoa, säännellä tietoa viranomaisten toimesta ja toisaalta teknologinen kehitys antaa mahdollisuuden levittää disinformaatiota entistä nopeammin ja tehokkaammin.

3.4.1 **Alustaekosysteemit, tiedon jäljitettävyys ja läpinäkyvyys**

Alustaekosysteemeillä tarkoitetaan tässä yhteydessä palvelualustoja, joilla on miljoonia käyttäjiä kuten esimerkiksi Twitter, Facebook, Instagram tai WeChat. Disinformaation levittämisen tavoissa, tiedon levittämisen nopeudessa ja laajan vaikutuksen tavoittelussa eri teknologioiden tai algoritmien hyödyntäminen ovat aivan keskeisessä roolissa. Näillä alustoilla on vapaasti voinut levittää haluamaansa tietoa, ilman että tiedon sisältöä olisi millään

lailla säännelty tai estetty. Vasta viime aikoina on lähdetty tehokkaammin puuttumaan sosiaalisen media botteihin, vihapuheeseen tai loanheittokampanjoihin. Tämän lisäksi on herätty myös kansalaisia aktiivisesti profiloiviin algoritmeihin. Algoritmit profiloivat meitä yhä tehokkaammin sosiaalisen käyttäytymisemme perusteella.

Mediassa on syytetty esimerkiksi Twitteriä siitä, ettei se tee riittävästi torjuakseen ikäviä ilmiöitä. Vastavoimana Twitterin käyttäjien lieveilmiöihin, on syntynyt esimerkiksi blocktogether.org-palvelu, joka antaa yhdelle käyttäjälle mahdollisuuden päättää muiden puolesta, milloin joku käyttäjä voidaan torjua. Tämä käyttäjä voi jakaa muille blokkauslistan, ja kun käyttäjä on estänyt jonkun, valuu tämä estolista kyseisen henkilön seuraajillekin. (Tivi 2018.) Twitter on myös itse lisännyt kaikkien käyttäjien mahdollisuuksia ilmiantaa käyttäjiä palveluntarjoajalle, blokata tai hiljentää itseltään käyttäjiä.

Bottien sataprosenttinen tunnistaminen Twitterin käyttäjäkunnasta on vaikeaa. Mediasta löytyy yhä useammin merkkejä laajamittaisista bottiverkostoista, jotka ovat liittyneet seuraajiksi. Esimerkkinä mahdollisesta automaattisesti luodusta bottiverkostosta voidaan mainita venäjänkielistien naisbottien lisääntyminen suomalaisten käyttäjien seuraajina. Erityisen suosittuja seurantakohteita näille boteille vaikuttavat olevan suomalaiset poliitikot, mielipidevaikuttajat, isot uutismediat ja niiden päätoimittajat. Nämä botit eivät ole twiitanneet mitään vaan ovat tyytyneet seuraajiksi, ja eivät todennäköisesti siksi ole haittaohjelman levittäjiä tai sivustojen mainostajabotteja. (Kortesuo 12.4.2018.) Tulevaisuudessa onkin mielenkiintoista seurata aktivoituvatko tämän tyyppiset bottitilit, vai onko ne luotu vain kokeilumielessä.

Suljettujen ekosysteemien merkityksen on uskottu kasvavan tulevaisuudessa. Tämä tulee koskemaan erityisesti WhatsApp-sovellusta, joka on globaalisti kaikkein käytetyin tiedonvaihtoon perustuva alusta. Kiinassa vastaavaa alustaa, WeChattiä, käyttää yli 963 miljoonaa käyttäjää vuoden 2017 tilastojen mukaan (Statista 2018). Suljettujen ekosysteemien sisältöjen seuraaminen muodostuu entistä hankalammaksi (Wardle & Derakhshan 2017, 75).

Alustaekosysteemejä tulisi kehittää siihen suuntaan, että ne mahdollistaisivat tiedon jäljitettävyyden ja läpinäkyvyyden. Lisäksi kuluttajien olisi hyvä tietää mitä tietoja heistä käytetään kohdennettuun verkkomainontaan, mitä tietoja käytetään poliittiseen mainontaan, sponsoroituihin sisältöihin tai mitä tietoa käyttäen algoritmit profiloivat meitä. Alustaekosysteemien osalta meillä pitäisi olla tietoa alustojen strategisista levittämismekanis-

meista eli kuten mielipidevaikuttajien palkkaamisesta tai robottien käytöstä markkinoinnissa (Euroopan komissio 2018, 7-9). Tarvitsemme tulevaisuudessa vastuullisempia tietoekosysteemejä, jotta tiedämme, miten tieto leviää verkossa.

Alustaekosysteemeille tulisi tulevaisuudessa kohdistaa seuraavanlaisia toimenpiteitä:

1. Vähennetään disinformaation levittäjien tuloja valvomalla mainossijoittelua ja rajoittamalla poliittista mainontaa
2. Varmistetaan sponsoroidun sisällön läpinäkyvyys
3. Tehostetaan valetilien sulkemista
4. Luodaan indikaattoreita, joilla käyttäjät voivat arvioida sisällön luotettavuutta
5. Otetaan käyttöön merkintäjärjestelmiä ja sääntöjä bottien havaitsemiseksi
6. Tarjotaan työkaluja disinformaation raportoimiseksi
7. Luodaan verkkopalveluihin sisäänrakennettuja disinformaation vastaisia
8. suojatoimia (Euroopan komissio 2018, 8-9.)

Verkkoalustat ovat lisänneet meidän kaikkien saatavilla olevan tiedon määrää. Teemme yhä enemmän ja nopeatempoisempia päätöksiä saatavilla olevaan tietoon perustuen. Internetin palveluiden ja monimuotoisuuden rajun lisääntymisen takia sääntely perinteisillä valvontatoimilla ei ole enää mahdollista. Yllä mainittujen toimenpiteiden voimaa lisäisi merkittävästi käyttäjien harjoittama itsesääntely. Internetin käyttäjien mahdollisuutta arvioida verkon sisältöä erilaisin indikaattorein tai kriteerein luotettavan sisällön löytämiseksi tulisi lisätä.

Verkkopalveluiden yksityiskohtaiset tiedot algoritmien käyttäytymisestä ja testimenetelmien kehittämisestä tulisi saattaa kuluttajien tietoon. Kuluttajien tulisi tietää miksi heille näytetään kulloistakin sisältöä. Olisi myös arvioitava sallitaanko luotettavien faktantarkistusorganisaatioille tai tiedeyhteisöille pääsy alustojen dataan algoritmien arvioimiseksi. (Euroopan komissio 2018, 9.)

3.4.2 **Faktantarkistuksen tulevaisuus**

Erilaisilla yhteiskunnallisilla toiminnoilla kuten esimerkiksi riippumattomalla faktantarkistuksella on merkittävä rooli sisällön uskottavuudelle. Faktantarkistus tulee olemaan yhä tärkeämpi osa median arvoketjua. Euroopassa tarvitaan vahvaa faktantarkastuksen verkostoa, jolla on kyvyt seurata disinformaation vaikutuksia, sen laajuutta ja erityisesti disinformaation leviämiseen käytettäviä tekniikoita yhteisen ymmärryksen luomiseksi. Eurooppalaisittain tarkasteltuna Suomessa hyvällä kuluttajan suojalla, medialukutaidolla ja korkealla koulutuksen tasolla on portinvartijan rooli disinformaation leviämisen ehkäisemiseksi. Mediassa leviävä tieto tarvitsee tulevaisuudessa luotettavia indikaattoreita tiedon läpinäkyvyyden ja luotettavuuden edistämiseksi. On kuitenkin selvää, että toimista huolimatta

vääristeltyä tietoa levittävät myös yksityiset henkilöt tai ryhmittymät erityisesti polarisoituneissa yhteiskunnissa. Näissä maissa disinformaation leviäminen tapahtuu sille otollisessa maaperässä. (Euroopan komissio 2018, 1-10.)

Faktantarkistuksen sekä erityisesti riippumattomuuden arvo ja merkitys disinformaation hallinnassa ja osana median arvoketjua tulee lähivuosina kasvamaan. Itsesääntely ei yksin riitä informaation alkuperän ja uskottavuuden tunnistamiseksi. Tarvitsemme faktantarkistusverkostoja, jotka analysoivat tiedon lähteitä ja tiedon levittämisen prosesseja.

Lisäksi akateemisten tutkijoiden riippumatonta roolia ja tulevaisuuden näkemyksellisyyttä tulisi hyödyntää disinformaation tekniikoiden, laajuuden ja vaikutusten arvioinnissa. Tutkimuksen avulla voitaisiin yksilöidä ja kartoittaa disinformaatiomekanismit. Disinformaatiomekanismien kartoittamisen jälkeen olisi kehitettävä objektiivisia ja luotettavia indikaattoreita lähteiden läpinäkyvyyden parantamiseksi. Myös uutismedian, viranomaisten sekä alustaekosysteemien olisi osallistuttava analysointiin kokoiskuvan saamiseksi. (Euroopan komissio 2018, 10-11.)

Suomalaisen Faktabaarin mukaan disinformaation tunnistamiseen liittyvien väitteiden valikoitumisprosessia tulee edelleen kehittää seuraavasti:

- Väitteiden valintaan ja rajaamiseen selkeät kriteerit.
- Kaikki esitettyjä väitteitä ei tarvitse tarkistaa vaan tarkistuksen laatuun tulee panostaa.
- Lähteiden käyttö ja seikkaperäinen merkitseminen on tärkeää.
- Väitteiden tarkastelussa pitää tuoda esiin niiden sisällöllinen asiayhteys osana laajempaa keskutelua.
- Kansainvälisten kriteereiden seuraaminen ja niiden tekeminen avoimeksi faktantarkistusprosessissa.
- Tutkijoiden ja toimittajien yhteistyötä tulee kehittää. Faktantarkistuksen asiantuntijoiden löytämistä helpottavia palveluita tulee yhdenmukaistaa ja kehittää.
- Resursseihin tulee panostaa. (Faktabaari 2018.)

3.4.3 **Teknologian hyödyntäminen tulevaisuudessa**

Teknologian tuomia uusia mahdollisuuksia disinformaation levittämiseen tulisi osata käyttää vastatoimiin eli disinformaation hallitsemiseen ja torjumiseen. Kaikkein haastavinta disinformaation torjunnassa on teknologian kiihtyvä muutosvauhti. Koneoppiminen, tekoäly, virtuaalitodellisuus ja lisätty todellisuus tulevat olemaan disinformaation jakamisen, uhrien profiloimisen ja tiedon muuttamisen työkaluja.

Äänen ja videokuvan reaaliaikainen muokkaaminen on ollut teknisesti mahdollista jo muutamia vuosia. Videokuvan muokkauksella pystytään muuttamaan myös kasvojen ilmeitä (Thies, Zollhofer, Stamminger, Theobalt & Nießner 2016, 2387-2395). Tekoälyn avulla

voidaan tunnistaa esimerkiksi suun liikkeiden ja muotojen algoritmit, joita voidaan käyttää videokuvan uudelleen muokkaukseen. Puhdasta ääntä voidaan puolestaan manipuloida kuvaa paljon helpommin, esimerkiksi ohjelmistoyritys Adobella on ollut pitkään saatavilla tuote, jolle voidaan tuottaa 10-20 minuutin pituisia äänimuunneltuja videoita (BBC News 2016). Yhdysvalloissa on jo tehty videoita, joissa tekoälyn avulla on jäljitelty muun muassa entisen presidentin, Barack Obama, suunliikkeet ja tehty manipuloitu video hänen puheestaan jossa ääni oli imitaattorin puhumaa (Fortune 2019).

Facebookin kehittäjät tekevät töitä lisätyn todellisuuden tuomiseksi kuluttajien saataville. Lisätty todellisuus tulee yhdistämään fyysisen ja digitaalisen maailman, jolloin ihmistä ohjaa hänen saamansa kokemus. Lisätty todellisuuden uskotaan tulevan lähelle fyysistä maailmaa tavalla, jonka Pokemon Go-peli opetti. Fyysiseen maailmaan tuodaan esimerkiksi virtuaalisia katuopasteita tai voimme luoda kolmiulotteisen mallin, vaikka höyryävästä kahvikupista ja luoda tunnelman siitä, ettemme syö aamiaista yksin. (The Guardian 2017.)

Keinoälyä voitaisiin tulevaisuudessa käyttää disinformaation tarkistamiseen ja tunnistamiseen. Tämä edellyttäisi toisaalta myös keinoälyyn kohdistuvaa valvontaa. Media-alustat voivat tulevaisuudessa kehittyä interaktiivisemmaksi ja tätä kautta kuluttajalle voitaisiin antaa mahdollisuus räätälöidä itse itselleen sopivia sisältöjä keinoälyn avulla. Lohkoketjuteknologia voisi tarjota tulevaisuudessa parempaa tiedon läpinäkyvyyttä ja jäljitettävyyttä. (Euroopan komissio 2018, 11-12.) Tekoäly voisi muokata paremmin oppivia algoritmeja, joita voisi hallita itse tai voisi tutkia datalähteiden paikansapitävyyttä. Tekoälyn, koneoppimisen ja virtuaalitodellisuuden mahdollisuudet ovat huikeat disinformaation torjumiseksi. Kuluttajan kannalta on tärkeää saada teknologia tuottamaan innovatiivisia ratkaisuja väärennetyn tiedon torjumiseksi.

4 Tutkimusmenetelmä, aineisto ja analyysi

Tässä luvussa esittelen disinformaation tunnistamisen prosessiin liittyvät kehittämisen vaiheet. Tutkimusmenetelmäksi on valittu tapaustutkimus. Opinnäytetyöhön kerätään aineistoa haastattelemalla ennalta valikoituja asiantuntijoita, järjestetään henkilöstön työpaja, etsitään tietoa www-sivustoilta, tutustutaan aihepiirin koti- ja ulkomaisiin tutkimuksiin, kirjallisuuteen, perinteisen median ja sosiaalisen median ulostuloihin.

4.1 Opinnäytetyön tarkoitus ja tutkimuskysymykset

Opinnäytetyön tarkoituksena on tuottaa ohjeistus disinformaation tunnistamiseen sekä kehittämisehdotuksia ja -ideoita tilannekuvatuotteen laadun ja luotettavuuden parantamiseen. Opinnäytetyön tutkimusaihe pohjautuu kolmeen peruskysymykseen: jotka kaikki vastaavat, miten jokin asia tulisi tunnistaa tai ohjeistaa.

Tutkimuskysymykset ovat:

1. Miten disinformaatio tunnistetaan jokapäiväisessä toiminnassa osana Kyberturvallisuuskeskuksen tilannekuvatuotantoa?
2. Miten disinformaation tunnistamisen tulisi vaikuttaa Kyberturvallisuuskeskuksen prosesseihin?
3. Miten Kyberturvallisuuskeskuksen henkilöstö voidaan ohjeistaa informaatiovaikuttamisen ja disinformaation varalta?

4.2 Tutkimusmenetelmän valinta

Tutkimusmenetelmän valintaan vaikuttaa se, että käsiteet informaatiovaikuttaminen ja disinformaatio ovat suhteellisen uusia ja niistä on saatavilla vähän suomalaista laaja-alaista tutkimustietoa. Aihe on vuorovaikutuksellinen ja sen kokonaisvaltainen ymmärtäminen kiinnostaa tekijää. Venäjään liittyvästä informaatiovaikuttamisesta löytyy erityisesti puolustussektorin tekemää tutkimusta jonkin verran, mutta pelkästään Venäjään liittyvä tutkimusmateriaali on tämän opinnäytetyön kannalta liian suppea.

Tapaustutkimus soveltuu hyvin tutkimusmenetelmäksi, koska informaatiovaikuttaminen on nykypäivän ilmiö. Kyseessä on kehittämishanke, jossa tutkitaan rajattua tapausta eli Kyberturvallisuuskeskuksen tilannekuvatuotannon prosessien kehittämistä, tiedon keräämistä sekä disinformaation aiheuttamia mahdollisia ongelmia tilannekuvatuotantoon. Tarkoituksena on myös tutkia informaatiovaikuttamisen käsitettä ja siihen liittyviä alalajeja.

Menetelmän valintaa puoltaa myös se, että opinnäytetyössä on tärkeää käyttää useita erilaisia tiedonhankintamenetelmiä, jotta informaatiovaikuttamisesta ja disinformaatiosta saadaan kokonaisvaltainen kuva (Ojasalo, Moilanen & Ritalahti 2014, 37). Tämä uuden asian äärellä oleminen tekee tapaustutkimuksesta arvokkaan (Kuluttajatutkimuskeskus 2005, 9). Tapaustutkimuksen valintaa tutkimusmenetelmäksi puoltaa myös se, että tutkimuksen kohteena on rajattu toiminto, jota tutkitaan käyttämällä eri menetelmiä. Tapaustutkimuksen avulla voi myös soveltaa teoriaa paremmin käytäntöön, jolloin Kyberturvallisuuskeskuksen tiedonhankinta - ja tilannekuvaprosessin eri osakokonaisuuksia voidaan liittää paremmin yhteen (Anttila 2005, 286-289). Lisäksi tapauksia pyritään selittämään ja kuvaamaan eri menetelmien avulla hankittujen tietojen avulla pääasiassa miten- ja miksi-kysymysten avulla (Yin 1994, 5-13). Tapaustutkimukselle on tyypillistä myös se, että tutkimuskohde on yksittäinen tapaus tai prosessi. Tapauksia ja prosesseja pyritään tutkimaan niiden luonnollisessa ympäristössä, jolloin tavoitteena on tapauksen tai prosessin piirteiden yksityiskohtainen tarkka, totuudenmukainen ja yksityiskohtainen kuvailu (Hirsijärvi, Remes & Sarjavaara 2004, 125–126).

Opinnäytetyön tutkimusmenetelmäksi olisi voinut valikoitua myös toimintatutkimus. Toimintatutkimuksessa organisaatiossa työskentelevät henkilöt tyypillisesti osallistuvat itse kehittämistyöhön ja kohteena on tyypillisesti organisaation ihmisen tai organisaation toiminnan muuttaminen (Ojasalo ym. 2014, 37). Toimintatutkimukselle luonteenomaista on henkilöstöä osallistava tutkimus, jossa ollaan kiinnostuneita, miten asioiden pitäisi olla ja tavoitteena on nykyisen todellisuuden muuttaminen (Ojasalo ym. 2014, 58).

Tapaustutkimukseen verrattuna toimintatutkimuksen tarkoitus on voimallisemmin muuttaa toimintaa, jossa tutkittavat ovat aktiivisesti itse mukana muutosprosessissa. Tämän kehittämishankkeen kannalta on järkevin kerätä tutkimukseen erilaisia näkemyksiä ja ideoita tahoilta, jotka ovat joko työelämässään tai tutkimuksessaan joutuneet käsittelemään informaatiovaikuttamista. Erilaisten ideoiden ja näkemysten kerääminen on osa monipuolista tiedonkeruuta, ja se mahdollistaa osaltaan tapaustutkimukselle tyypillisen laajapohjaisen analyysin (Yin 1994, 1-3).

Konstruktiivinen tutkimusmenetelmä ei sovellu tähän opinnäytetyöhön. Sen on tavoitteena ratkaista ongelma luomalla jokin konkreettinen tuote esimerkiksi tietojärjestelmä tai uudistaa verkkosivusto. Muutos kohdistuu konkreettiseen tuotteeseen eikä esimerkiksi henkilöstön toimintatapaan. (Ojasalo ym. 2014, 37–38.)

4.3 Tiedonkeruun menetelmät ja aineistot

Tapaustutkimus soveltuu erilaisten aineistojen ja aineistolähteiden käyttämiseen rinnakkain. Erilaisten aineistojen käyttöä samassa tutkimuksessa kutsutaan aineiston triangulaatioksi (Kuluttajatutkimuskeskus 2005, 42). Aineistolähteitä voivat olla esimerkiksi teemahaastattelut, strukturoidut tai puolistrukturoidut haastattelut, media-aineisto, erilaiset dokumentaatiot, esitteet tai havainnoinnit. Käyttämällä laajaa aineistopohjaa, saadaan monipuolinen näkemys aiheesta sekä tutkimuksen kannalta paras lopputulos. Toisaalta laajaalaisesta aineistopohjasta voi löytyä ristiriitaisuuksia, ja niitä tuleekin käsitellä optimistisesti mielenkiintoisten kysymysten avaajina. (Kuluttajatutkimuskeskus 2005, 41-42.)

Opinnäytetyö on osa Kyberturvallisuuskeskuksen asiatuntijatyön kehittämistä. Asiantuntijatyön kehittämiseen soveltuvat hyvin yhteisölliset menetelmät. Omasta työyhteisöstä saatujen kokemusten perusteella tähän soveltuvat parhaiten henkilöstön yhteiset työpajat, jossa kehitettävää prosessia ja ohjeistusta voi testata sekä jalostaa. Useimpien menetelmien rinnakkaiskäyttö luo varmuutta sekä helpottaa kehitystyöhön liittyvää päätöksentekoa (Ojasalo ym. 2014, 40).

Opinnäytetyön aineisto muodostuu haastatteluista ja erilaisesta dokumentaatiosta sekä työpajan annista. Työpajan tarkoituksena on informaatiovaikuttamisen ja disinformaation ymmärryksen lisääminen haastatteluista saadun tietopohjan avulla sekä vastata opinnäytetyön tutkimuskysymyksiin mediasta valikoitujen esimerkkien pohjalta.

Opinnäytetyön tutkimuskysymysten tiedonkeruu aloitetaan kirjallisuuslähteitä tutkimalla. Käsitteiden avaamisessa käytetään erilaisia kansallisia ja kansainvälisiä tutkimuksia, printtimedian ja sosiaalisen median kirjoituksia, erilaisia www-sivustojen dokumentteja sekä mahdollisuuksien mukaan kirjallisuuslähteitä.

4.4 Haastatteluaineiston kerääminen

Tietopohjaa laajennan valitsemalla haastateltavaksi joukon asiantuntijoita, jotka ovat tutustuneet työelämässään informaatiovaikuttamiseen ja disinformaatiosta. Haastattelujen tarkoitus on lisätä ymmärrystäni Suomeen kohdistuvasta informaatiovaikuttamisesta ja disinformaatiosta ilmiöinä sekä keinoista niiden havainnointiin. Haastattelut vastaavat osin tutkimuskysymykseen, miten disinformaatio tunnistetaan jokapäiväisessä toiminnassa osana Kyberturvallisuuskeskuksen tilannekuvatuotantoa. Lisäksi haastattelut vastaavat laajemman näkökulman kautta osin kysymykseen, miten disinformaation tunnistamisen vaikuttaa Kyberturvallisuuskeskuksen prosesseihin.

Haastattelut toimivat osaltaan opinnäytetyön tietoperustana. Informaatiovaikuttamiseen ja disinformaation levittämiseen ei ole löydettävissä laajaa kansallista teoriapohjaa. Haastattelujen tehtävänä on tässä työssä kuvata taustaa ja jäsentää opinnäytetyön tarkoitusta.

Haastateltavani ovat ennalta tuntemiani valtiohallinnon henkilöitä ja kyberturvallisuuden tutkijoita, joilla on laaja ja monipuolinen tausta kyberturvallisuuden ja tietoverkoissa tapahtuman vaikuttamisen ilmiöihin. Valitsemani henkilöt olivat työelämässään tutustuneet informaatiovaikuttamiseen, disinformaatioon, kyberturvallisuuteen, Kyberturvallisuuskeskukseen sekä sen toimintaan. Haastattelujen teemoina ovat informaatiovaikuttamisen ja disinformaation tunnistaminen yksilönä ja yhteisönä. Haastattelut suoritetaan haastateltavien anonymiteettiä kunnioittaen. Anonymiteetista ja luottamuksellisuuden säilymisestä pidetään huolta myös tietoja julkistettaessa (Kuula 2006, 201-207).

Pidin tärkeänä sitä, että haastateltavat saavat aloittaa haluamastaan teemasta. Mielestäni tämä lisää haastattelujen sujuvuutta ja luonnollisuutta sekä saa esille myös uusia kysymyksiä, joita en mahdollisesti osaa ensiarviolta esittää. Haastattelut tehdään osin avoimena haastatteluna. Avoimen haastattelun tarkoituksena on selvittää haastateltavan mielipiteitä, käsityksiä ja ajatuksia siten, että ne tulevat aidosti esille keskustelun aikana (Hirsjärvi, Remes & Sarjovaara 1997, 205). Avoimia haastatteluita voidaan kutsua myös syvä- ja eliitin haastatteluksi, jolloin voidaan tarkastella paremmin menneitä tapahtumia, heikkoja signaaleja ja arkaluonteisia asioita (Aaltola & Valli, 2007, 44). Kysymyksen tai kysymysten ollessa jäsentymätön, on haastateltavan helpompi puhua hänelle tärkeistä asioista (Syrjälä & Numminen, 1988, 103).

Jos avoin haastattelu ei vaikutta johtavan tutkimuksen kannalta tarvittavan tiedon hankintaan, olen valmis siirtymään kesken haastattelun myös puolistrukturoituun haastattelurunkoon. Puolistrukturoidun haastattelurungon avulla voin ohjata haastattelua ennalta suunniteltuihin teemoihin, avoimen haastattelun eksyessä teeman kannalta epäolennaisiin asioihin (Hirsjärvi & Hurme 2001, 47). Mietin teeman tueksi myös tarkkoja kysymyksiä, jotka voidaan esittää eri järjestyksessä eri haastateltaville haastattelun kulkua myötäillen. Tietojen luotettavuuden käsittely on tärkeä aihe opinnäytetyössä, koska tietojen tarkistaminen on valeuutisten vastakohta sekä keino informaatiovaikuttamiseen ja disinformaation tunnistamiseen.

Haastattelut taltioidaan nauhoittamalla ne. Haastatteluaineiston analysointivaihe tapahtuu litteroinnilla. Nauhoitetut haastattelut puretaan tekstinkäsittelyohjelmalla, jolloin pystyn perehtymään aiheeseen syvällisesti jo litterointivaiheessa. Kuuntelen nauhoitukset useaan

kertaan lävitse, jolla tarkistan kirjoitetun tekstin paikkansa pitävyyden. Analyysin teko alkaa jo ensimmäistä haastattelua purkaessa. Seuraavien haastattelujen aikana kokoan samansuuntaisia teemoja jatkotyöhön.

5 Asiantuntijahaastattelut

Haastattelin opinnäytetyötäni varten kuutta eri asiantuntijaa kesä-elokuussa 2018. Heillä kaikilla on laaja-alaista tietämystä sekä Kyberturvallisuuskeskuksen toiminnasta että informaatiovaikuttamisesta ja osa heistä työskentelee Kyberturvallisuuskeskuksessa. Haastattelut tehtiin avoimena haastatteluna kasvokkain haastateltavien kanssa. Haastattelut kestivät noin tunnista kahteen ja ne äänitettiin myöhempää analysointia varten.

Haastatteluiden tavoitteena oli saada mm. näkemyksiä siitä, mitä informaatiovaikuttamisella ja disinformaatiolla tarkoitetaan, miten informaatiovaikuttamista tehdään, mitkä ovat sen kohteet, motiivit ja mahdolliset eri tekniikat. Lisäksi tavoitteena oli löytää haastatteluiden avulla keinoja disinformaation tunnistamiseen ja miten sitä voitaisiin hyödyntää Kyberturvallisuuskeskuksen toiminnassa. Haastatteluista oli tarkoitus saada myös ideoita ja ajatuksia keskuksen henkilökunnalle järjestettävää työpajaa varten.

Haastattelun aluksi kertasin vielä, miksi haastattelut tehdään ja mistä opinnäytetyössäni on kysymys. Haastatteluiden avulla sain taustatietoa opinnäytetyön tietoperustaa varten. Haastattelun tulokset on äänitteiden analyysien perusteella referoitu pääteemoiksi opinnäytetyön kohtiin 5.1.1-5.1.3.

5.1.1 Informaatiovaikuttaminen ja disinformaation kohteet

Haastateltavien mukaan väärällä informaatiolla eli disinformaatiolla tarkoitetaan epätarkkaa tai manipuloitua tietoa jota levitetään tarkoitushakuisesti. Asiassa ei sinänsä ole mitään uutta, sillä se on ollut propagandan väline jo vuosisatoja, mutta se on ollut myös viimeaikaisten valeuutisten lähtökohta. Informaatiovaikuttaminen on toimintaa, jolla pyritään järjestelmällisesti vaikuttamaan yleiseen mielipiteeseen, ihmisten käyttäytymiseen, päätöksentekijöihin ja sitä kautta yhteiskunnan toimintakykyyn. Tarkoituksena on vaikuttaa päätöksentekoon Suomessa ja EU:ssa, lamauttaa päätöksentekokykyä tai ainakin heikentää sitä, lisäämällä epäluuloa päättäjiä kohtaan.

Informaatiovaikuttamisen keinoja ovat esimerkiksi väärien tai harhaanjohtavien tietojen, disinformaation, levittäminen sekä painostaminen, mutta myös sinänsä paikkaansa pitävän tiedon tarkoitushakuinen käyttö. Vaikuttamista voidaan pitää strategisena toimintana, jonka tavoitteena on saada kohde tekemään itselleen haitallisia päätöksiä tai toimimaan omaa etuaan vastaan. On myös huomioitava, että informaatiovaikuttaminen voidaan jakaa sisäiseen ja ulkoiseen vaikuttamiseen. Sisäisestä vaikuttamisesta on esimerkkinä Yhdys-

valtojen sisäinen tilanne, jossa presidenttiä myöten, pyritään sosiaalisessa mediassa vaikuttamaan kansalaisten mielipiteisiin erittäin voimakkaasti ja sen vastapuolena on vapaa media, joka pyrkii kertomaan asioita journalistisista lähtökohdista. Ulkoisena vaikuttamisena voidaan pitää eri vaaleihin kohdistunutta vaalivaikuttamista, joissa ulkoiset tahot ovat pyrkineet saamaan vaaleissa itselleen mieluisan lopputuloksen.

Useat haastateltavat toivat esille, että yleisesti ottaen informaatiovaikuttamisessa pyritään henkisen tilan hallintaan. Mediatila pidetään hallussa ohjatuilla strategisilla narratiiveilla, monikanavaisella viestinnällä ja kohdeyleisön myötävaikutuksella. Keinotekoisia ja sepitteellisiä sisältöjä ei kaihdeta ja tarina on totuutta tärkeämpää. Voidaan myös sanoa, että totuudella ei itse asiassa ole oikeastaan mitään väliä disinformaatiota levitettäessä.

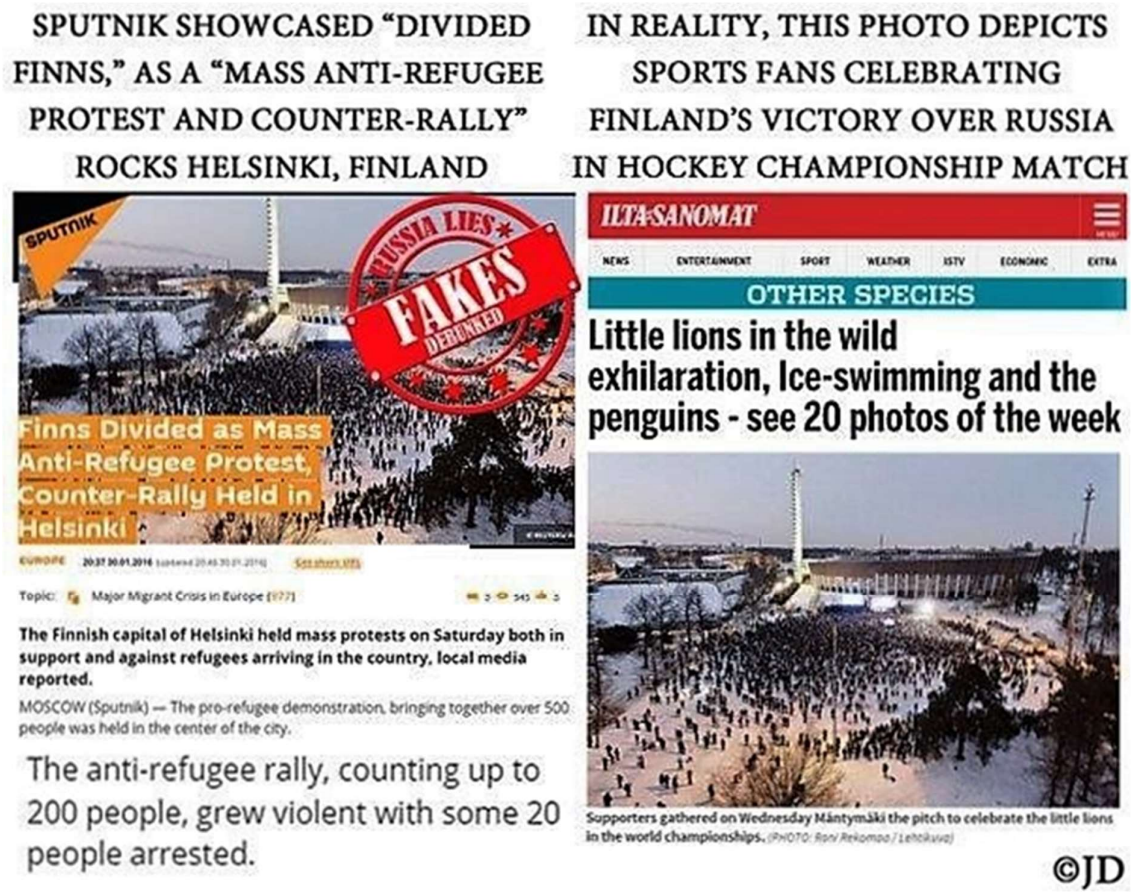
Kaikkien haastateltavien mukaan informaatiovaikuttamisella voi olla erilaisia kohderyhmiä. Jos kohderyhmänä on laaja yleisö, kohdennetaan disinformaatio kertomuksiin, joita jaetaan laajasti tai ovat muuten laajasti saatavilla. Kohdennettaessa vaikuttaminen ryhmiin vaikuttaa kohteen valinnassa muun muassa väestötilastolliset asiat kuten ikä, tulot ja koulutus ja yksilöihin kohdistuvassa vaikuttamisessa valintaperusteina voivat olla esimerkiksi persoonallisuuspiirteet, käyttäytymismallit ja poliittiset mielipiteet.

5.1.2 **Disinformaation levittämisen teknologiset keinot**

Haastateltavien mukaan informaatiovaikuttamisen ja disinformaation levittämisen tekniikat kehittyvät jatkuvasti teknologisen kehityksen seurauksena. Useasti tekniikat ovat neutraaleja eivätkä ne ole lähtökohtaisesti hyviä tai huonoja. Eri tekniikoita voidaan käyttää joko informaatiovaikuttamiseen ja disinformaation levittämiseen tai hyväksytyillä tavoilla ja avoimesti.

Kahden haastateltavan mukaan on huomioitava, että digitaaliset alustat ovat muuttaneet tapaa, jolla väärä informaatio leviää. Virheellinen sisältö voi koostua erilaisista manipuloiduista elementeistä kuten tekstit, kuvat, äänet ja videot. Tällä tarkoitetaan tietoa ilman tosiasiallista perustaa ja joka on julkaistu yleisön harhaanjohtamiseksi, uskoakseen sen olevan laillinen. Esimerkiksi väärennetty sähköposti poliitikolta saatetaan tuottaa ja vuotaa lehdistölle heikentämään kyseisen poliitikon uskottavuutta. Manipuloimalla viestiä tekstin, valokuvan, videon tai äänen sisällöllä ja samalla poistaen tai muuttaen kertomaan sen eri viestiä. Oikean sisällön käyttö, jota on esitelty erillisellä asialla, tosiasiallisesti muodostaa asian pettävällä tavalla.

Yhden haastateltavan mukaan vääristelty uutinen saattaa käyttää kuvia erillisestä tapahtumasta osoitukseksi sen olemassaolosta. Hänen mukaansa alla oleva uutisointi on esimerkki, jossa kuvaa käytettiin kertomaan suomalaisten jakautuneen ja järjestäneen massamielenosoituksia silloista pakolaistilannetta vastaan. Todellisuudessa kuva oli otettu suomalaisesta yleisöjuhlasta, jotka järjestettiin olympiastadionin kupeessa Suomen voitettua jääkiekon nuorten maailmanmestaruuden vuonna 2016 (kuva 6).



Kuva 6. Kuvan käyttö harhautukseen (Russialies 2016)

Useat haastateltavat toivat esiin, että yksi informaatiovaikuttamisen tekniikka on erilaisten teknologisten keinojen yhtäaikainen hyväksikäyttö. Teknisesti osaavat henkilöt voivat manipuloida verkon kautta tiedon sisältöä ja sen kulkua. Verkon kautta voidaan suorittaa manipulointia automatisoiduilla algoritmeilla ja ihmisten sekä automaation yhdistelmillä. Teknologinen hyväksikäyttö käyttää usein teknologista etua suorittamaan melko perinteisiä informaatiovaikuttamisen keinoja kuten tekaistut identiteetit, disinformaatio ja väärennys. Teknologisten innovaatioiden hyväksikäytön alue kehittyy nopeammin kuin ihmisen kyky analysoida ja ymmärtää sen potentiaalia ja seurauksia. Koneoppiminen ja tulevaisuudessa myös tekoäly vähentävät lingvistisiä esteitä entisestään, joka taas helpottaa globaalia informaatiovaikuttamista ja disinformaation levittämistä.

Yleisin teknologian hyväksikäytön keino on haastateltavien arvion mukaan botit. Boteilla voidaan käyttää vahvistamaan kommentteja ja sosiaalisen median näkyvyyttä helpottamaan sitoutumista "todellisilta" käyttäjiltä. Tämä saattaa antaa vaikutelman sosiaalisesta hyväksymisestä, joka taas vetoaa tarpeeseen sosiaaliselle yhdenmukaisuudelle. Orgaanisesti luodut alaryhmät, jossa ihmiset ovat tekemisissä mielipiteitään samanlaisten kanssa, ovat olemassa sekä verkon kautta että tosielämässä. Esimerkiksi äänestäjät saattavat kääntyä tietyn median käyttäjiksi tiedon hankkimista varten, seurustella etupäässä vertaistensa kanssa ja osallistua keskusteluihin foorumeilla saman lailla poliittisesti suuntautuneiden ihmisten kanssa. Tätä voidaan käyttää hyväksi vahvistamaan ja levittämään tietynlaista tietoa tietyille ihmisryhmille.

Useat haastateltavat pitivät sosiaalisen median vitsauksena väärennettyjä identiteettejä. Henkilön tai henkilöiden hallitsemat huijaritilit eivät paljasta niiden todellista identiteettiä. Vääriä identiteettejä voidaan käyttää esimerkiksi osallistumaan väittelyihin verkkoyhteisöissä ja tarvittaessa kahta eri tiliä voidaan käyttää matkimaan väittelyn molempia osapuolia ja ohjaamaan verkkoyhteisön keskusteluja sekä mielipiteitä. Samanlaisia väärennettyjä identiteettejä käytetään myös verkkokaupoissa, joissa tuotteiden palkatut arvostelijat jakavat mielipiteitä ja kokemuksia eri tuotteista. Vastaavalla tavalla toimivat henkilöt, jotka väittävät olevansa esimerkiksi koulutettuja lääkärin ammattiin, mutta eivät sitä todellisuudessa ole.

Verkkoyhteisön keskustelujen aggressiivisimpina ja myös tarkoitushakuisimpina toimijoina pidetiin trolleja. Trollit levittävät tietoa, kyllästyttävät tietyt verkkosivustot kommenteillaan ja saattavat jopa mustamaalata tai ahdistella muita kommenteillaan. Trollaus voi olla organisoitua laitosmaista toimintaa, mutta sitä toteuttavat myös yksilöt autonomisesti. Trollaukselle on ominaista, että trollaaja laittaa levitykseen kiistanalalaisen viestin synnyttääkseen reaktioita. Jos "haasteet" eivät toimi, trollaaja voi tekeytyä eri henkilöksi joka vaihtoehtoisesti tukee heitettyä "haastetta" tai haastaa sen niin liioitellusti, että saa aikaan reaktioita verkkoyhteisössä. Kun trollaaja on saanut aikaan keskustelua, jatkaa se keskustelua haastamalla tai tukemalla systemaattisesti eri kommentteja. Verkossa käytävän keskustelun ylläpitämiseksi trollaaja vaihtelee keskustelun sävyjä muun muassa ironiasta aina loukkauksiin saakka.

Kaksi haastateltavaa toi esiin koneoppimisen ja tekoälyn, jotka ovat tuoneet myös informaatiovaikuttamiseen ja disinformaation levittämiseen uuden ilmiön, niin kutsutun "deepfaken". Deepfakessa henkilön kasvoja muutetaan digitaalisesti ja algoritmien avulla

jäljitellään ja väärennetään videolla olevaa ääntä, suun liikkeitä tai molempia jolloin kuka tahansa saadaan uskottavasti sanomaan mitä tahansa.

5.1.3 Yhteenveto disinformaation levittämiseen käytetyistä tekniikoista

Haastatteluissa esiin tulleiden käsitysten ja eri tekniikoiden osalta voidaan todeta, että minkään yksittäisen tekniikan käyttö ei välttämättä ole merkki informaatiovaikuttamisesta ja disinformaation levittämisestä, mutta useamman tekniikan yhtäaikainen käyttö yhdistettynä kohderyhmäanalyysiin saattaa antaa viitteitä informaatiovaikuttamisesta ja disinformaation levittämisestä. Yksi haastateltava kuvasi kyberin ja disinformaation teknistä suhdetta seuraavasti "Se on kuin öljyputki, jossa kyber on putki ja virtaava öljy on putken sisällä kulkevaa disinformaatiota".

Haastatteluiden sisältö auttoi minua merkittävästi työpajan rakenteen suunnittelussa ja työpajan esimerkkitapausten valinnassa. Haastatteluissa käytiin läpi muun muassa suurvaltojen tekemää tietojen vääristelyä sekä väärennettyjä sosiaalisen median tilien käyttöä. Näistä sain ideat esimerkkitapauksiini. Haastattelut vahvistivat käsitystäni siitä, että työpajassa ei voitu keskittyä pelkästään yksittäisiin esimerkkitapauksiin vaan aihetta tuli pohjustaa ja käsitellä laajemmin työpajaan osallistuvien kanssa, jotta heidän ymmärryksensä informaatiovaikuttamisesta ja disinformaatiosta lisääntyy. Haastattelut helpottivat myös esimerkkitapausten valintaa, koska haastatteluissa nousi esille erilaisia disinformaation levittämisen tapoja.

6 Työpaja: disinformaation tunnistaminen

Työpajan tarkoituksena oli löytää vastauksia opinnäyteyön keskeisimpään kysymykseen: miten disinformaatio tunnistetaan ja sitä kautta arvioida, miten tunnistamisen mallit vaikuttavat Kyberturvallisuuskeskuksen olemassa oleviin tilalannekuvatuotteiden prosesseihin. Työpajassa arvioitiin esimerkkitapauksia uuden testimallin avulla sekä käytiin läpi faktantarkistuksen oppeja.

6.1 Työpajan tavoite

Henkilöstölle järjestettiin työpaja, jossa he saivat tutustua viiteen erilaiseen esimerkkiin median uutisoinnista. Esimerkkejä käytiin läpi alustavan kybertapausten arvioinnin testimallin avulla. Ohjeisto oli luonnosteltu käyttämällä kysymysten laadintaan omaa kokemustani alalta, kirjallista tietopohjaa ja tekemiäni haastatteluja. Lisäksi alustavaa ohjeistoa verrattiin faktantarkistussivustolta Faktabaari löytyneeseen oppeihin. Työpajan tavoitteena oli esimerkkien avulla löytää vastauksia opinnäytetyön tutkimuskysymyksiin, yleisen ymmärryksen lisääminen disinformaatiosta, käytännön oppimista faktantarkistamisesta sekä tiedonhankkimisen arvioinnista.

6.2 Työpajaan valmistautuminen

Työpajan suunnittelu alkoi periaatteessa jo ennen opinnäytetyöni aiheen hyväksyntää, sillä olin jo pidemmän aikaa pohtinut mielessäni opinnäytetyöni mahdollisten löydöksien testausta. Opinnäytetyön edistyessä ajatukseni työpajan järjestämisestä vaihtui välillä tulosten kevyempään testaukseen, mutta lopulta päädyin kuitenkin pitäytymään lopullisessa suunnitelmassa, opettajan kanssa käytyjen ohjauskeskusteluiden perusteella.

Ohjauskeskusteluiden jälkeen ideointi ja suunnittelutyö jatkuivat kotona. Käytännössä tehtäviini kuuluivat työpajan sisällön tarkempi suunnittelu, työpajan materiaalin valmistelu ja koehenkilöiden valitseminen työpajaan. Vaikeimmaksi tehtäväksi työpajan suunnittelussa osoittautui sellaisten kansantajuisten esimerkkien löytäminen internetin syövereistä, joiden todenperäisyyttä voitiin tarkastella ja arvioida. Ajatukseni oli löytää aiheita, jotka olisivat kaikille jo entuudestaan tuttuja mediasta ja sen lisäksi tavoitteena oli saada mukaan esimerkki sosiaalisesta mediasta.

Päädyin kahteen uutiseen, joiden faktatieto oli todennäköisesti työpajaan osallistuneiden tiedossa ja järkyttävyydellään ylittäneet myös heidän omat uutiskynnyksensä. Näiden kah-

den uutisen osalta tavoitteena oli etsiä tietoa siitä, miten uutisten sisältö muuttui lähtötilanteesta ja sitä kautta herättää myös keskustelua työpajaan osallistuneiden kesken. Lisäksi valitsin keskustelun aiheeksi bottitilin tunnistamisen, Twitter-viestinnän Imatran ampumavälikohtauksesta ja median uskottavuuden arvioinnin liittyen suomalaisen rautatieinfran myyntiin Norjaan.

Valitsin työpajaan henkilöstöstä työntekijöitä, jotka eivät ole aikaisemmin tutustuneet informaatiovaikuttamisen tai disinformaation käsitteeseen. Tällä menettelyllä varmistin, että opinnäytetyön tulokset saadaan kirjattua mahdollisemman ymmärrettävästi asiaa tuntemattomankin luettavaksi.

Esimerkkitehtävien valinnan jälkeen pystyin itse testaamaan paljonko kunkin tehtävän suorittamiseen menisi aikaa. Toki itse valittujen tehtävien suorittaminen on huomattavasti nopeampaa kuin sellaisten henkilöiden, jotka perehtyvät tehtäviin ensimmäistä kertaa. Arvioin myös, että mitä paremmin työpajan esitysmateriaali tukee tehtävien suorittamista, sitä nopeammin tehtävistä suoriuduttaisiin. Päädyin työpajan aikataulun suunnittelussa siihen, että varasin lopullisesta aikataulusta tupla-ajan siihen nähden jonka itse käytin esimerkkitehtävien suorittamiseen. Jos aikaa kuluisi vähemmän, voitaisiin myös tehtävien nostamista ajatuksista keskustella enemmän ja toisaalta, jos aikataulu tuntuisi tiukalta, voisin neuvomalla edistää aikataulussa pysymistä.

Power Point- esityksessäni (liite 1) oli kerrottu työpajan tarkoitus, työpajaan sopivien tutkimuskysymysten arviointi sekä aikataulu. Kerroin myös opinnäytetyöni sen hetkisistä näkemyksistä, kuten mitä disinformaatio on, millaisia toimijoita ja tarkoitusperiä disinformaation "pelikentällä" toimii ja miten faktantarkistusta mielestäni kannattaisi testimallin avulla tehdä.

Työpajaan osallistujien valinta oli myös pitkän pohdinnan tulos. Opinnäytetyöni tarkoituksena oli parantaa sellaisten ihmisten tietoutta disinformaatiosta, joilla ei ole tietoperustaa asiasta. Alun perin tarkoituksenani oli valita koehenkilöt Kyberturvallisuuskeskuksen henkilöstöstä, mutta päädyin valitsemaan henkilöt Viestintäviraston muusta henkilöstöstä, koska oletin näin saavani paremmin tietoa testimallin käytännön soveltuvuudesta. Koehenkilöiden valintaperusteena oli se, että heillä ei ole ollut tapana sen kummemmin tarkastaa uutisten sisältöä ja olisivat sosiaalisessa mediassa ainakin Twitterin tai Facebookin käyttäjiä.

Sen jälkeen, kun vaihdoin koehenkilöryhmän valintaperusteita Kyberturvallisuuskeskuksesta muuhun Viestintäviraston henkilöstöön, mietin kahta vaihtoehtoa siihen, miten saan

työpajaan koehenkilöitä. Vaihtoehtoina olivat sähköpostikysely tai kahvipöytäkeskustelu. Ajankäytöstä johtuen, päädyin ensi kokeilemaan kahvipöytäkeskusteluita, joissa johdattelin keskustelua yleiseen uutisten lukemiseen, median toimintaedellytyksiin Yhdysvalloissa ja sosiaalisen median käyttöön. Onnekseni jo parin keskustelun jälkeen sain "valittua" viisi henkilöä työpajaan ja jotka jo ensi kysymällä olivat aiheesta kiinnostuneita. Sopivaksi ajankohdaksi valikoitui 25.10.2018 klo. 12.30-16.00. Työpajan ajankohdan kiinnittämisen jälkeen tarkensin vielä hieman suunnitelmissani ollutta alkuperäistä aikataulua. Olin alun perin suunnitellut työpajan aikatauluksi neljä tuntia, mutta 30 minuutin lyhentymisen takia muodostui lopullinen aikataulu seuraavanlaiseksi:

Esittäytyminen ja orientaatio	klo. 12.30-13.30
Tauko	klo. 13.30-13.45
Esimerkkitehtävien ratkominen	klo. 13.45-15.30
Jälkikäsittely	klo. 15.30-16.00.

6.3 Työpajan kuvaus

Työpaja starttasi käyntiin siihen varatussa tilassa suunniteltuun aikaan ja paria pientä myöhästymistä lukuun ottamatta kaikki työpajaan osallistujat saapuivat paikalle ajallaan. Tehtävien suorittamista varten kaikilla oli mukana myös tietokoneet ja matkapuhelimet, kuten olin pyytänyt.

Aloitimme työpajan nopealla esittelykierroksella, jossa kaikki saivat kertoa nimensä ja omasta mielestä päivän mielenkiintoisimman uutisen. Tämän jälkeen kertasin iltapäivän sisällön ja aikataulun, joka oli jo valmiiksi näkyvillä tilassa olevalla näytöllä.

Lähdin taustoittamaan informaatiovaikuttamisen kokonaisuutta ottamalla ensimmäiseksi esimerkiksi vaaleihin vaikuttamisen. Informaatiovaikuttaminen sanana oli usealle tuttu, mutta suurin osa ei ollut esimerkiksi ajatellut sitä, että vaaleihin vaikuttaminen on samalla puuttumista demokraattiseen päätöksentekoon ja samalla voidaan horjuttaa yhteiskunnallista vakautta ja poliittista tasapainoa. Tässä vaiheessa kaikki mielestäni syttyivät aiheeseen ja saivat lyhyen kuvauksen informaatiovaikuttamisen yhteiskunnallisesta merkityksestä. Kävimme myös lyhyen keskustelun siitä millä tavoin viranomaista kohtaan yleistä luottamusta voitaisiin heikentää ja kuinka helposti mieliimme voidaan vaikuttaa median huomionhakuisilla otsikoilla. Yksi työpajaan osallistuvista kertoi, että hänen arjessaan sosiaalinen media on koko ajan läsnä älypuhelimen kautta ja näin olemme kaiken aikaa vaikutuksille alttiita.

Esittelin määritelmät informaation eri lajeista ja sen jälkeen keskustelimme disinformaatiosta. Kysyin, kuinka moni oli mielestään tunnistanut mediasta disinformaatiota? Kolme viidestä kertoi välillä epäilevänsä Yhdysvaltain presidentti Trumpiin liittyvän uutisoinnin todenperäisyyttä. Näistä kaksi nosti esiin erityisesti Trumpin ja Pohjois-Korean johtajan Kim Jong-Unin sekä Trumpin ja Venäjän presidentti Putinin tapaamisiin liittyvät uutisoinnit. Erityisesti hämmennystä keskusteluissa herätti presidentti Trumpin Yhdysvaltain mediaan lausumat kommentit ja mahdollisesti jo samana päivänä vastakkaiset kommentit hänen omalla Twitter-tilillään.

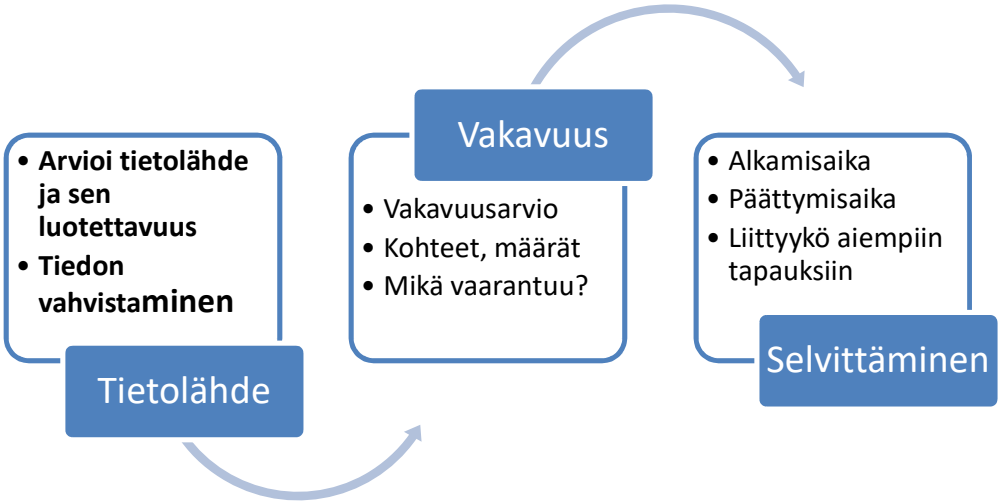
Seuraavaksi keskustelimme disinformaation levittämisen kanavista. Kaikille olivat käsitteenä tuttuja internetin botit erityisesti Twitterin osalta. Kaksi työpajaan osallistuneista kertoi ilmi-antaneensa Twitterille useamman kerran botteja. Keskustelu lähti ihan uudelle tasolle vauhtiin, kun avasin internetin algoritmien käyttöä. Internetin liikenteestä on suurin osa muuta kuin ihmisen itsensä tuottamaa dataa. Suurimmalle osalle oli tuttua sosiaalisessa mediassa meitä profiloivat mainosalgoritmit. Yksi osallistujista kertoi siitä, että erään verkkokaupan tietyt tuotteet tuntuvat tulevan hyvin usein alennukseen sen jälkeen, kun niitä on katsellut muutaman kerran tai että Facebook osaa ehdottaa hyvinkin täsmällisiä mainoksia.

Tulevaisuuden alustojen kuten virtuaalitodellisuuden ja keinoälyn mukaan otto vaikuttamisen kanaviin osalta herätti todella vilkasta keskustelua ja minun tuli jarruttaa sitä, että pääsisimme nykymallin ja testimallin kybertapausten arviointeihin käsiksi.

6.3.1 **Nykymalli kybertapausten arvioinnissa**

Kävimme työpajassa seuraavaksi läpi sitä, miten nykymallissa virastossa arvioidaan kybertapaukset. Kerroin, että tällä hetkellä kybertapahtuman luonteesta riippuu, kuinka nopeasti se on tarve arvioida ja käsitellä se tarkemmin vahinkojen minimoimiseksi ja laadukkaan tilannetiedon jakamiseksi kumppaneille (kuva 7). Kerroin, että kaikkein korkeimmalle prioriteetille tällä hetkellä asetetaan seuraavat ilmiöt:

- Viestintäverkkojen ja -palvelujen häiriöt: Palvelun käyttäminen on häiriintynyt tai estynyt ja käyttäjät havaitsevat ongelman.
- Palvelunestohyökkäys: Palvelu ei ole käytettävissä tai on erittäin hidas käyttäjille
- Tietovuoto: Tietomurron kautta saadut tiedot on vuodettu julkisuuteen ja välittömästi hyödynnettävissä.
- Haittaohjelma: Haittaohjelma leviää verkkosivuston tai sähköpostin kautta.
- Huijaukset: Phishing- tai muu esim. sähköpostitse tai tekstiviestein leviävä huijaus-kampanja.



Kuva 7. Tapauksen arviointi ja käsittely

Arvioinnin alkuvaiheessa on tärkeää varmistaa, että tieto on luotettavaa ja tiedon alkuperä on vahvistettu. Nykymallissa tiedon alkuperää arvioidaan pääasiassa sillä, että tieto on tullut tunnetulta lähteeltä kuten vastinkumppanilta yrityksessä tai valtiohallinnon organisaatiossa. Keskustelimme siitä että, tapaukset, joissa tapahtuma koskettaa laajasti kansalaisia tai elinkeinoelämää täytyy arvioida myöskin heti. Uhkaavat tapaukset, joista ei ole selkeää varmuutta edellyttävät usein selvityksiä toimenpiteiden suorittamiseksi ja asiasta riittävän täsmälliseksi tiedottamiseksi. Kaikki meistä olivat sitä mieltä, että selvittämisen osalta on hankalaa todentaa tapahtumien alkamis- ja päättymisaikaa ja varsinkin sitä liittyykö kybertapahtuma johonkin laajempaan kokonaisuuteen. Yksi työpajaan osallistuneista kysyi todennäköisyyttä siitä, ovatko nämä prioriteettitapaukset sellaisia, joiden avulla voidaan jakaa disinformaatiota tai joiden vaikutusten arviointia voidaan käyttää disinformaation levittämiseen. Totesin, että erityisesti palvelunestohyökkäyksissä, tietovuodoissa tai vakoilutapauksissa voidaan julkisuudessa syyttää tänä päivänä valtioita tai toisen maan valtiollisia organisaatioita.

Jatkoimme tämän jälkeen faktantarkistuksen pariin ja esittelin Faktabaarin tänä vuonna uudistettuja oppeja. Kävimme opit pikaisesti esityksestäni läpi eikä meillä ollut aikaa kuin käydä yksi keskustelu. Pohdimme omaa opinnäytetyötäni peilaten miten tarkistettavien väitteiden valikoitumisprosessia voisi kehittää. Emme vielä tässä vaiheessa osanneet ottaa kantaa siihen, miten saataisiin selkeät kriteerit väitteiden valintaan ja rajaamiseen.

6.3.2 **Testimalli kybertapausten arvioinnissa**

Lähdimme pohtimaan työpajassa seuraavaksi luonnostelemaani testimallia disinformaation tunnistamiseen ja lähteiden luotettavuuden arviointiin. Kerroin, että omaan kokemukseeni perustuen faktantarkistus onnistuu jossain määrin ilman suurempaa tietoteknistä osaamista noudattamalla hyvin pitkälle "maalaisjärkeä" ja selvittämällä muutamia keskeisiä asioita.

Kerroin siitä, että usein Viestintäviraston Kyberturvallisuuskeskus on toimittajien faktantarkistuksen kohde tai lähde, varsinkin kun on kyse kybertapahtumista, joilla on yhteiskuntaan tai kansalaisiin kohdistuvia vaikutuksia. Lähdimme käymään alla olevaa listaa läpi.

1. Ole terveen epäluuloinen
2. Tarkista julkaisija
3. Tarkista toimittajien nimet ja toimituksen osoitetiedot (oikeita vai keksittyjä), Google ja erilaiset rekisterit ovat tähän varsin hyvä väline
4. Tärkeää lukea koko juttu ei pelkkää otsikkoa ja ingressiä (sisällön tulisi vastata otsikkoa)
5. Tarkista jutun lähteet
6. Tarkista mahdolliset puhutut lainaukset
7. Mikäli jutussa mainitaan tutkimus, tarkista onko tutkimusta olemassa
8. Mahdollisten numeeristen tietojen tarkistus
9. Tarkista uutisen kielioppi ja sävy (herjaukset, jonkun henkilön tikkuun nostaminen jne.)
10. Onko uutinen oikeasti ajankohtainen vai onko sen tarkoitus "kaivella" vanhoja
11. Tarkista sivuston osoitteen oikeellisuus (valesivustot jäljittelevät tunnettuja osoitteita)
12. Vievätkö julkaisun linkit "oikeille" sivustoille

6.4 Työpajan case-esimerkit

Tauon jälkeen lähdimme käymään esimerkkejä läpi siten, että esittelin uutisen ja pyysin jokaista viiden minuutin ajan käymään läpi esimerkin uutista testimallin kysymyksien avulla. Kaikilla oli mukanaan tietokoneet ja kännykät, joten tilaisuudesta muodostui samalla harjoitus internetin erilaisten hakujen tekemiseen.

6.4.1 **Malesialaisen MH17 matkustajakoneen alas ampuminen**

Ensimmäisessä esimerkissä keskityimme malesialaisen MH17 matkustajakoneen alas ampumiseen liittyvään ristiriitaiseen uutisointiin, joka liittyi BBCn dokumenttiin vuodelta 2016 (kuvat 8 ja 9).

25.04.2016

BBC:n dokumentti väittää:

Ukrainalaishävittäjä ampui MH17:n alas

Tänään klo 16:43

Malesiaan matkalla ollut matkustajakone ammuttiin alas Ukrainassa pari vuotta sitten. Nyt BBC väittää, että koneen ampui alas ukrainalainen taistelukone.

Kone hajosi pieniksi palasiksi. AP

Hollannista matkaan lähtenyt Malesian lentoyhtiön Boeing 777 -matkustajakone räjähti kappaleiksi Ukrainan itäosissa heinäkuussa 2014. Turmassa kuoli 298 ihmistä.

Virallisen raportin mukaan koneen ampui alas venäläisvalmisteinen Buk-ohjus, joka laukaistiin Venäjän tukemien kapinallisten hallitsemalta alueelta.

Nyt toukokuun alussa esitettävä BBC:n dokumentti esittää rohkeita väitteitä, joiden mukaan koneen olisikin ampunut alas ukrainalainen taistelukone. Silminnäkijät väittävät

Kuva 8. (maanpuolustus.net 2016)

UUTISET

Uutiset | Ulkomaan uutiset

BBC tyrmää väitteet MH17-dokumentista - Ukrainalainen hävittäjä ei voinut pudottaa matkustajakonetta

25.04.2016 klo 16:43 (muokattu 25.04.2016 klo 16:43)

Kremlille myötämielisten medioiden mukaan BBC:n tuleva dokumentti vahvistaa, että ukrainalainen hävittäjä ampui alas MH17-koneen. BBC kiistää tämän.

Kuva 9. (Iltalehti 2016)

Kerroin osallistujille, että toinen esillä olevista kuvista on keskustelupalstalta ja toinen Iltalehden verkkosivuilta. Pyysin heitä etsimään tietoa kyseisestä uutisesta ja sitä, onko keskustelupalstalla ollut tieto oikeaa vai onko keskustelupalastalla disinformaatiota.

Kahta osallistujaa alkoi heti epäilyttää Iltalehden uutisen todenperäisyys, koska kuvan mukaan uutista oli jo oikaistu samalla minuutilla, kun sen ensimmäinen versio oli julkaistu. Aloitimme Iltalehden uutisen etsimisen Googlen avulla ja hyvin pian kaikki osallistujat olivat 25.4.2016 julkaistun uutisen äärellä. Lähes kaikki ihmettelivät aluksi, mikä uutisessa oikeastaan on epäilyttävää, kunnes he lukivat vihjeestäni uutisen loppuun ja huomasivat, että keskustelupalstalta löytyvä uutinen oli todellakin julkaistu alun perin Iltalehdessä.

Hämmästelimme yhdessä sitä, miksi tiedot uutisen oikaisusta ovat vasta sen lopussa ja kaiken lisäksi kellonaika poikkesi uutisen alusta olevasta muokkausajasta yli kahdella tunnilla, sillä uutisen lopussa kerrottiin otsikon oikaisun tapahtuneen kello 18.59. Kaikki totesivat, että selkeä oppi on kiireestä huolimatta lukea uutiset kokonaisuudessaan.

6.4.2 **Imatran ampumistapaus**

Toinen esimerkki oli Twitter-viestinnästä, joka liittyi Imatralla vuonna 2016 sattuneeseen ampumistapaukseen (kuva 10). Twitterissä levisi viesti, jonka mukaan ampuja olisi ollut puolustusvoimien kantahenkilökuntaa ja uhrit venäläisiä.

Kuva 10. (Twitter 2016)

Pyysin niitä henkilöitä, joilla on Twitter-tili etsimään kyseistä tiliä. Hyvin nopeasti havaittiin, että tiliä ei enää ole. Sen jälkeen aloimme etsiä internetistä uutisointia tapahtumasta ja erityisesti siitä, kuinka nopeasti viranomaiset olivat pystyneet oikaisemaan Twitterissä levinneen virheellisen tiedon ja pyysin myös osallistujia miettimään voisiko levinnyt tieto olla disinformaatiota.

Löysimme aiheesta paljonkin uutisointia, jotka sijoittuivat keskiyön tienoilla tapahtuneen ampumisen jälkeiseen aamuun. Ensimmäiset tiedot viranomaisen oikaisusta liittyen uhrien kansalaisuuteen ja ampujaan löytyivät vasta seuraavalta aamupäivältä. Kolme osallistujaa löysi myös uutisen trollitehtaasta, jonka tekona twiittiä pidettiin. Hämmästystä herätti viranomaisten hidas reagointi, vaikka kaikki olivat sitä mieltä, että totta kai tällaisissa tapauksissa omaisille pitää saada tieto tapahtuneesta ennen tiedottamista ja myös viranomaisten pitää varmistaa julkisuuteen annettavat tiedot. Kaikki olivat kuitenkin sitä mieltä, että yleisen mielipiteen muokkaus ja disinformaation leviäminen, jollaisena kyseistä twiittiä pidettiin, on mahdollista, mikäli viranomainen ei oikaise väärää tietoa riittävän nopeasti.

6.4.3 läkkäät miehet karkasivat vanhainkodista

Kolmas esimerkki liittyy saksalaisiin seniorimiehiin, jotka uutisen mukaan karkasivat vanhainkodistakodista hevimusiikki festivaaleille (kuva 11). Tarkoituksena on etsiä oikaisemattoman uutisen oikaistu versio ja totuus seniorimiesten seikkailusta.

Kuva 11. (Radio Nova 2018)

Pyysin ensin kaikkia etsimään esimerkissä olevasta Radio Novan uutisesta. Uutista etsiessään kaksi osallistujaa muisti lukeneensa uutisen hauskasta tapahtumasta, jossa vanhukset pääsivät verestämään nuoruuden muistoja. Kaikki löysivät uutisen, jonka jälkeen pyysin heitä etsimään samaa uutista muista lähteistä.

Hämmästys oli melkoinen, kun kaikissa muissa löydetyissä lähteissä uutinen oli oikaistu ja todellisuudessa mielenterveyspotilaat olivat löytyneet karkumatkan jälkeen pienestä kylästä huonossa kunnossa. Laajalle suomenkin mediassa levinnyt uutinen oli oikaistu suhteellisen hitaalla aikataululla, vaikka saksalaisessa mediassa tiedot oli oikaistu huomattavasti nopeammin. Jälleen herätti huomiota se, että osassa uutisia oikaisu oli vasta uutisen lopussa, eikä heti uutisen alussa. Tosin uutisten alussakin olevia oikaisuja löytyi tällä kertaa. Pohdintaa herätti myös se, että mikäli oikaisut olisivat aina uutisen alussa, johtaisiko se siihen, että uutisia ei luettaisi kokonaisuudessaan vai herättäisikö se jopa suurempaa mielenkiintoa uutista kohtaan. Kaksi osallistujaa moitti Radio Novaa, koska muistelivat kanavan mainostaneen vastuullista journalismia televisiomainoksissa.

6.4.4 **Suomen rautatieinfran myyminen Norjaan**

Neljännen esimerkin kautta pyritään arvioimaan tietyn median luotettavuutta. Uutisen mukaan Suomi pyrkii vähentämään merenkulun päästöjä ja on myymässä rautatieinfran Norjaan (kuva 12)

Kuva 12. (Nykysuomi 2018)

Uutinen herätti ja heti alkuun hilpeyttä, koska työskentely liikenne- ja viestintäministeriön hallinnonalalla pitää työntekijänsä varsin hyvin tietoisena ministeriön ja ministerin eri tavoitteista. Tosin yksi osallistujista totesi, että miksipä ei, sillä hän muisti lukeneensa uutisen jonka mukaan maailman 15 suurinta rahtilaivaa saastuttaa enemmän kuin koko maailman autoliikenne yhteensä.

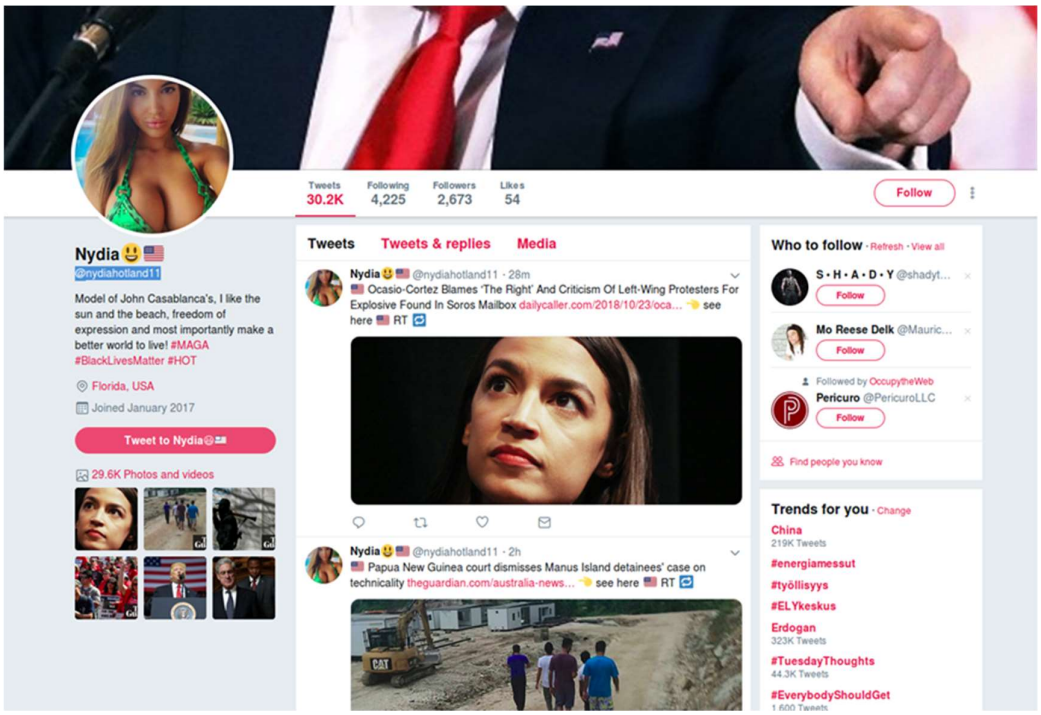
Etsimme Nykysuomen sivuilta kyseisen uutisen ja tutkimme myös muita sivustolta löytyviä uutisia. Uutisia pidettiin varsin hyvin kirjoitettuina, vaikka niiden sisältö ei aina herättänyt-kään luottamusta. Lisäksi sivujen "halpa" visuaalinen ilme ja yhteystietoina käytetyt gmail-sähköpostiosoitteet herättivät epäilyksiä.

Tämän jälkeen etsimme vielä Googlen avulla mitä Nykysuomesta kerrotaan. Varsin nopeasti selvisi, että kyseistä julkaisua pidetään yleisesti valemediana ja äärioikeistolaisena. Kolme henkilöä totesi kuitenkin, että sisältö on niin uskottavasti kirjoitettua, että mikäli

muuten ei seuraa uutisia saattaisi Nykysuomen uutisointia pitää uskottavana ja sitä kautta mielipiteenmuokkaajana.

6.4.5 **Bottitilin tunnistaminen**

Viidennessä esimerkissä oli tarkoitus tunnistaa Twitterin bottitili (kuva 13) ja bottitileille tunnusomaisia piirteitä. Olin saanut kyseisen bottitilin arvioitavaksi Kyberturvallisuuskeskuksen työyhteisöstäni.



Kuva 13. (Twitter 2018)

Pyysin niitä henkilöitä, joilla oli Twitter-tili kirjautumaan palveluun tämän esimerkin ajaksi. Esittelin @nydiahotland1-nimisen Twitter-tilin tunnustietoja, koska osalla työpajaan osallistuneista ei ollut omaa tiliä, eikä yhdellä henkilöistä ollut lainkaan sosiaalisen median tiliä. Kävimme läpi, milloin tili on perustettu, kuinka paljon tili on twiitannut, mistä löytää tilin tiedot ja katsoimme, minkälaisia kuvia tili on twiitannut.

Tässä vaiheessa ei ollut enää aikaa omatoimiseen tutkimiseen ajankäytön takia, ja sen vuoksi lähdimme käymään esityksessäni ollutta kalvoa bottitilin tunnistamisesta läpi yhdessä. Ensimmäisenä kiinnitimme huomiota tilin twiittien erittäin suureen lukumäärään, joka oli 30200 kappaletta ja lähes jokainen twiitti on sisältänyt kuvan tai videon. Tili oli avattu tammikuussa 2017. Siitä laskimme, että tili oli twiitannut 22 kuukauden aikana noin

1400 kertaa kuukaudessa ja noin 50 kertaa päivässä. Twiittien jokapäiväinen lukumäärä viittaa hyvin vahvasti siihen, että kyseessä on bottitili. Suurin osa twiiteistä oli edelleen lähetettyjä twiittejä, joissa ei ollut mitään omaa sisältöä. Arvioimme, että seurattavien tilien 4225 kappaletta ja seuraajien 2673 kappaletta olivat puolestaan melko normaaleja, jos ne suhteuttaa twiittien lukumäärään ja tilin nuoreen ikään.

Bottitili on yleensä ilman kuvaa ja profiilin kuvaus voi olla lyhyt tai linkki jollekin muulle sivustolle. Tässä tilillä oli profiilikuva sekä kuvaus henkilöstä, jota kuva esittää. Lähdimme arvioimaan kuvaa Googlen kuvahaulla. Kuvahaun avulla löysimme lähes samanlaisen kuvan naishenkilöstä, joka oli venäläinen bikinimalli. Tämän perusteella totesimme, että tilin kuva ja profiilin kuvaus ovat ristiriitaiset. Esittelytekstin perusteella kyseessä yhdysvaltalaisen John Casablanca yrityksen malli. Kyseinen yritys on kyllä mallitoimisto, mutta kyseisen mallin kuvaa ei ole löydy tämän yrityksen palveluksesta.

Tämän esimerkin osalta olimme kaikki yhtä mieltä siitä, että kyseessä on bottitili. Tilin luomiseen on käytetty aikaa, ja arvelimme että tilin tarkoituksena saattaisi olla kerätä seuraajia ja käyttää heitä mahdollisesti jatkossa tiedon jakamisen lähteinä. Esityksessäni olleet bottitilin tunnistamisen malli toimi tässä esimerkissä oikein hyvin.

6.4.6 **Jälkikäsittely**

Työpajan päätteeksi pidettiin jälkikäsittely, debriefing, missä kukin vuorollaan sai kertoa omista kokemuksistaan ja ajatuksistaan työpajasta. Sain työpajasta paljon positiivista palautetta ja osallistujat pitivät työpajassa käytetyistä esimerkeistä sekä pitivät työpajaa mielenkiintoisena ja opettavaisena. Työpaja oli kestoltaan kolmen ja puolen tunnin mittainen ja huolimatta ennen työpajaa ajoittuneeseen lounastaukoon osallistujat jaksoivat hyvin keskittyä tekemiseen koko työpajan ajan. Yksi työpajan lomassa pidetty nopea kahvitauko oli tarpeellinen.

Suurimmalla osalle sanat informaatiovaikuttaminen ja disinformaatio olivat tuttuja, mutta niiden merkitystä ja vaikuttamismekanismia yhteiskuntaan ei tunnettu. Suurin osa työpajaan osallistujista olivat myös Twitterin ja Facebookin käyttäjiä, mutta heille ei ollut tullut mieleen se, miten tehokkaita disinformaation levittämisalustoja kyseiset sovellukset ovat. Internetin botit olivat kaikille tuttuja kyberturvallisuuden ilmiöiden kautta. Sen sijaan trollitehtaiden olemassaolo ja järjestäytynyt toiminta bottien ja meitä arvioivien algoritmien osalta oli uutta tietoa. Erityisesti toiminta sosiaalisessa mediassa puhututti, esimerkiksi identiteetin kaappaaminen ja viranomaisen nimissä väärän tiedon jakaminen vahingoittaisi merkittävissä määrin kansalaisten tuntemaa luottamusta viranomaisia kohtaan.

Pohdimme myös suomalaisen median faktantarkistusherkkyyttä ja kykyä koskien ukrainalaishävittäjän tekemää alas ampumista ja siihen liittynyttä väärennettyä kuvaa suomalaisessa uutisoinnissa. Yksi keskeisimmistä kysymyksistä lienee se, miten tunnistaa ja rajata aiheet joihin kohdistuu erityistä syytä suorittaa faktantarkistusta.

Tavallisen kansalaisen tietoisuus disinformaatiosta on melko kaukana jokapäiväisestä arjesta ja kestää pitkään, että yksittäinen henkilö lähtisi ihmettelemään uutisointia tai tarttuisi epäilen johonkin omassa sosiaalisen median ympäristössä olevaan uutisointiin. Totesimme, että suomalaiseen yhteiskuntaan kuuluu pitkälti luottamus kaikkeen mediaan. Tämä on näkynyt Kyberturvallisuuskeskuksen uutisoimissa eri tyyppisissä huijauskampanjoissa koskien sitä, miten hyväuskoisia me olemme tilanteessa, joissa esimerkiksi sosiaalinen media tarjoaa meille voittoja tai veronpalautuksen etukäteisnostoa.

Yhtenä välittömänä kehittämisajatuksena työpajassa nousi ajatuksena esille se, että voisiko vastaavanlaista esimerkkien pohjalta rakennettua perehdytystä tehdä viraston sisäisessä intranetissä. Lisäksi työpaja oli myös kaikkien mielestä hyvä harjoitus oppia käyttämään internetin hakupalveluja järjestelmällisemmin, erityisesti kaikille tuli uutena kuvahakujen tekeminen tiedon etsinnän tukena.

Keräsin työpajan lopuksi kaikilta muutaman oivalluksen ja palautetta. Kirjasin esitykseni loppuun työpajastani saamat oivallukset. Työpajan lopun "kevennyksenä" näytin vielä esimerkin deepfakesta. Manipuloidulla videolla nähdään, kuinka tekoälyn avulla on jäljitelty entisen presidentin, Barack Obama, suunliikkeet ja on tehty video hänen puheestaan, jossa ääni oli imitaattorin puhumaa. Video herätti lähinnä epäuskoisuutta siitä, mihin tulevaisuudessa voi uskoa. Työpajan lopputuloksia käsitellään tämän opinnäytetyön yhteenvedossa luvussa 7.

7 Yhteenveto ja pohdinta

Tässä luvussa arvioidaan opinnäytetyön kysymysten toteutumista sekä esitetään kehitysideoita Kyberturvallisuuskeskuksen tilannekuvatuotannon prosesseihin, arvioidaan opinnäytetyön onnistumista sekä esitetään aihioita jatkotutkimuskysymyksiksi.

Lisäksi olen sisällyttänyt tähän lukuun työpajan (luku 6) keskeisimmät opit ja kehittämiskohteet. Yhteenvedossa on huomioitu opinnäytetyössä kerätty tietoperusta kansallisista ja kansainvälisistä artikkeleista, aihepiirin aikaisemmista tutkimuksista, aihepiiriä koskevista ja sivuavasta kirjallisuudesta, haastatteluista, työpajasta sekä tekijän työelämäkokemuksesta.

7.1 Vastaukset tutkimuskysymyksiin

Etsiessäni kirjallista materiaalia opinnäytetyötä varten, en törmännyt tutkimuksessa enkä julkaisuissa opinnäytetyöni kaltaisiin disinformaation tunnistamis- ja prosessikysymyksiin. Haastattelujen perusteella nostamani kysymykset ovat juuri tähän aikaan sopivia ja suunnaltaan oikeanlaisia, ja joihin ei ole löydettävissä yksiselitteistä vastausta muun muassa informaatiovaikuttamisen moniulotteisuuden ja disinformaation näkymättömyyden ja tuntemattomuuden vuoksi.

Arvioin seuraavaksi asettamiani tutkimuskysymysten löydöksiä.

1. Miten disinformaatio tunnistetaan jokapäiväisessä toiminnassa osana Kyberturvallisuuskeskuksen tilannekuvatuotantoa?

Kysymyksen osalta voidaan todeta, ettei informaatiovaikuttamisen ja disinformaation olemassaoloa tunnisteta riittävällä tasolla. Informaatiovaikuttamisen ja disinformaation tunnistamista pohdittiin työpajan jälkipuinnissa. Informaatiovaikuttaminen ja disinformaatio eivät ole viraston henkilöstön jokapäiväisessä tekemisessä läsnä, ja sen tunnistaminen vaatii tekemisessä hereillä oloa ja kokonaisuuksien hahmottamista. Työpajan avulla sain kuitenkin osoitettua käytännössä, että varsin yksinkertaisilla esimerkeillä ja testimallin kysymyksillä ja faktantarkistuksen opeilla voidaan parantaa henkilöiden valveutuneisuutta disinformaation tunnistamisessa.

Disinformaatioon päästään käsiksi paremmin virastotasolla, jos Kyberturvallisuuskeskuksen henkilöstölle jaettaisiin entistä enemmän tietoa ja koulutusta informaatiovaikuttamisesta yleensä ja lisäksi vaikuttamisen sen kohteista ja miten sillä pyritään vaikuttamaan.

Asiantuntijahaastatteluissa tuli esiin se, että disinformaation avulla yritetään voimakkaasti vaikuttaa yleiseen mielipiteeseen eikä ole syytä olettaa, ettei tämän kaltaista vaikuttamista tapahtuisi myös jossakin määrin Suomessa. Osa asiantuntijoista otti myös sen esille, että myös paikkaansa pitävää tietoa voidaan käyttää tarkoitushakuisesti, esimerkiksi aikaansaada tilanteita, joissa viranomainen tekisi itselleen haitallisia päätöksiä. Asiantuntijat pitivät vaalivaikuttamista kaikkein merkittävimpänä huolena. Samaan huolestuneen sävyyn disinformaation vaikutusten merkityksestä keskusteltiin myös henkilöstölle järjestetyssä työpajan jälkipuinnissa. Kaikilla viranomaisilla ei ole riittävää kykyä tunnistaa disinformaatiota. Suomen mediassa asia on melko vähäisellä huomiolla, joka tarkoittaa sitä, että kansalaisilla on vielä heikompi kyky ymmärtää asian merkityksellisyys. Kaikki haastateltavat olivat sitä mieltä, että kansalaisten kouluttautuminen informaatiovaikuttamisen käsitteeseen sekä disinformaation tunnistamiseen on yhä tärkeämpää tulevaisuudessa.

Uskoisin, että disinformaation tunnistamisen kouluttaminen omassa työyhteisössäni ja laajempi tietämys siitä, että disinformaatiolla pyritään vaikuttamaan ihmisten käyttäytymiseen, yhteiskunnan toimintaan ja päätöksentekoon loisi yhä valveutuneemman henkilöstön ja kollektiivisen kyvykkyyden ennakoida ja tunnistaa asioita. Toisaalta tarvitaan myös viranomaisen omia proaktiivisia toimia jakaa asiasta tietoa kansalaisille ja kuluttajille medialukutaidon vahvistamiseksi.

2. Miten disinformaation tunnistamisen tulisi vaikuttaa Kyberturvallisuuskeskuksen prosesseihin?

Tämä on ehdottomasti vaikein opinnäytetyön kysymyksistäni. Disinformaation tunnistamiseen liittyy olennaisesti kyky erottaa uutisvirrasta ne asiat, joita tulisi seurata ja tarkistaa. Tähän kysymykseen olisi huomattavasti helpompi vastata, jos kyseessä olisi median toimituskunnat, jotka itse luovat uutisvirtaa yhdistämällä saatavilla olevaa materiaalia. Uuden tiedon tuottamisessa on oleellista tarkistaa esimerkiksi aiheeseen liittyvät lähteet, luvut, kuvat ja julkaisut. Kysymys jakaantuukin kahteen eri kokonaisuuteen: omaan tilannekuvatuotantoon ja sen sisällön faktantarkistukseen sekä haastavampaan osaa eli muiden tuottaman uutisvirran disinformaation tunnistamiseen.

Omassa tilannekuvatuotannossa voidaan ottaa käyttöön testimallin kysymykset. Ne ohjaavat kirjoittajaa käyttämään faktantarkistusta tilannekuvatuotteiden kirjoittamisprosessin alkuvaiheessa. Toisaalta testimallin käyttöönotto kannustaa henkilöstöä käyttämään hakukoneita, digitaalisen median kuvien vertailumalleja tai erilaisia algoritmeja entistä tehokkaammin ja taitavammin. Asiantuntijahaastatteluissa tuotiin vahvasti esille se, että informaatiovaikuttamisen ja disinformaation levittämisen ytimessä ovat erilaisten teknologisten

keinojen yhtäaikainen hyväksikäyttö. Haastatteluissa lähes kaikki totesivat, että teknologista kyvykkyyttä tulee käyttää myös disinformaation tunnistamiseen. Tulevaisuudessa koneoppimista ja keinoälyä voidaan yhä monipuolisemmin käyttää vääristeltyjen sisältöjen löytämiseen ja tunnistamiseen.

Mielestäni Kyberturvallisuuskeskuksen tilannekuvatuotteiden luonti vastaa jossain määrin journalistin työtä faktantarkistuksen osalta. Myös meidän julkaisema tilannekuva tulee olla totuudenmukainen ja sen luontiin tarvittavat tiedot on tarkistettava mahdollisemman hyvin. Suhtaudumme journalistien tavoin tietolähteisiimme kriittisesti, jos ne eivät kuulu omaan luottamusverkostoomme tai kansainvälisiin vastinpareihimme.

Tämän vuoksi näen tärkeänä, että myös meillä virastossa tilannekuvatuotteiden kirjoittamisprosessin alkuun, aiheen tunnistamisen jälkeen, on lisättävä faktantarkistusprosessi, joka tarkoittaa aiheeseen liitettävien tietojen tarkistamista testimallin kysymysten avulla. Testimallin käyttöönotto tulisi ottaa käyttöön heti aihepiiriin kouluttamisen jälkeen, viimeistään vuoden 2019 alusta alkaen.

Käyttöön otettavan mallin kysymykset ovat seuraavat:

1. Ole terveen epäluuloinen
2. Tarkista julkaisija
3. Tarkista toimittajien nimet ja toimituksen osoitetiedot (oikeita vai keksittyjä), Google ja erilaiset rekisterit ovat tähän varsin hyvä väline
4. On tärkeää lukea koko juttu ei pelkkää otsikkoa ja ingressiä (sisällön tulisi vastata otsikkoa)
5. Tarkista jutun lähteet
6. Tarkista mahdolliset puhutut lainaukset
7. Mikäli jutussa mainitaan tutkimus, tarkista onko tutkimusta olemassa
8. Mahdollisten numeeristen tietojen tarkistus
9. Tarkista uutisen kielioppi ja sävy (herjaukset, jonkun henkilön tikkuun nostaminen jne.)
10. Onko uutinen oikeasti ajankohtainen vai onko sen tarkoitus "kaivella" vanhoja
11. Tarkista sivuston osoitteen oikeellisuus (valesivustot jäljittelevät tunnettuja osoitteita)
12. Vievätkö julkaisun linkit "oikeille" sivustoille

Kysymyksen toinen osuus eli informaatiovaikuttamisen ja disinformaation tunnistaminen ulkoisesta uutisvirrasta vaatisi jatkokehitystä. Toki tähänkin kohtaan voidaan hyödyntää haastatteluissakin nousseita teknologisia keinoja.

Oikein lähteiden ja tiedon löytäminen internetistä realisoituu varsinkin silloin, kun tutkimme kansalainvälisiä tapauksia ja tarvitsemme itse luotettavaa tilannekuvaa avoimista tietolähteistä. Toisaalta tarkemman tiedon etsimiseen avoimista tietolähteistä hyödynnetään

myös erilaisia mediaseurantaohjelmia. Tähän osuuteen voidaan tulevaisuudessa hyödyntää asiantuntijahaastatteluissakin nousseita uusia teknologisia kykyjä kuten koneoppimista ja keinoälyä. Näiden lisäksi mielestäni viranomaisen tulee seurata myös tiiviisti esimerkiksi Euroopan komission erilaisia aloitteita alustaekosysteemiin kohdistuviksi toimenpiteiksi. Erityisen kiinnostavana näen aloitteet indikaattoreista, joilla käyttäjät voisivat itse arvioida sisältöjen luotettavuutta tai aloitetta siitä, miten saataisiin verkkopalveluihin sisäänrakennettuja disinformaation vastaisia suojatoimia.

3. Miten Kyberturvallisuuskeskuksen henkilöstö voidaan ohjeistaa informaatiovaikuttamisen ja disinformaation varalta?

Tähän kysymykseen löytyi selkeä vastaus ja toimintamalli. Opinnäytetyön tuloksena syntyi testimalli, joka koettiin työpajassa erittäin toimivaksi ja hyödylliseksi. Testimallista syntyy henkilöstölle ohjeistus, jonka koulutus pitää aloittaa Kyberturvallisuuskeskuksen mahdollisimman nopeasti tilannekuva- ja yhteistyöverkostot -ryhmälle sekä tilannekeskus-ryhmälle. Muiden Kyberturvallisuuskeskuksen henkilöstön osalta koulutus tulee ottaa mukaan vuoden 2019 toiminnan suunnitteluun.

Lisäksi työpajassa syntyi erinomainen idea siitä, että työpajan kaltaisia ratkomistehtäviä ja testikysymysten käyttöä voitaisiin käyttää laajemminkin perehdytysmateriaalina viraston sisäisessä intranetissä. Tämän tyyppinen hyvä harjoitusmateriaali ohjaisi henkilöstöä myös käyttämään internetin hakupalveluja järjestelmällisemmin, erityisesti kuvahakujen tekemistä tiedon etsinnän tukena. Tiedon ollessa koko organisaation saatavilla tapahtuu yhdessä oppimista ja uudenlaista ajattelua aiheen ympärillä.

Tämän lisäksi meidän olisi syytä viranomaisena ottaa vahvempi rooli medialukutaidon edistäjänä ja tuottaa kansalaisille enemmän tietoa informaatiovaikuttamisesta ja disinformaation levittämistavoista ja kanavista. Voisimme myös harkita omiin tilannekuvatuotteisiimme lisättäväksi oma-aloitteisesti indikaattoreita lähteiden luotettavuudesta, esimerkiksi siitä, että tieto on saatu meille Kyberturvallisuuskeskuksen luottamusverkoston kautta ja pidämme sitä kokemuksemme mukaan luotettava.

Tulevaisuudessa Kyberturvallisuuskeskuksen uuden henkilöstö rekrytointivaiheen testinä voitaisiin arvioida vastaavanlaisten tapausten kautta, miten hyvin henkilö tuntee disinformaation tunnistamiseen liittyvät kokonaisuudet.

7.2 Kehitystoimenpiteet Viestintävirastossa

Opinnäytetyöni tutkimuskysymykset vastaavat suomalaiseen yhteiskuntaa koskettavan uuden ilmiön, disinformaation, tunnistamiseen. Viestintäviraston Kyberturvallisuuskeskuksen henkilöstön osalta aihe ja ilmiö ovat tuttuja, mutta vain harva on työssään tullut tehneeksi faktantarkistusta.

Työni ja siihen liittyvät kehittämistoimet liittyvät keskeisesti Viestintäviraton henkilöstön työelämän ymmärryksen, taitojen ja prosessien kehittämiseen. Disinformaation tunnistaminen voidaan liittää osaksi Kyberturvallisuuskeskuksen tilannekuvantuotannon prosessia, jolloin omien tilannekuvatuotteidemme laatu ja luotettavuus paranevat.

Disinformaation tunnistamisen osalta Viestintävirastossa toteutetaan seuraavat kehittämistoimenpiteet:

1. Kyberturvallisuuskeskuksen henkilöstö kokonaisuudessaan koulutetaan disinformaation tunnistamiseen lisäämällä aihe toimialan toiminnansuunnitteluun vuodelle 2019.
2. Kouluttamisen jälkeen kybertapausten testimalli otetaan käyttöön tilannekuvatuotannossa tilannekuva- ja yhteistyöverkostot -ryhmässä. Toteutetaan osana ryhmän vuoden 2019 toiminnansuunnittelua.
3. Viestintäviraston sisäisessä intranetissä julkaistaan tämän opinnäytetyön harjoitusesimerkit ja vastaukset. Samassa yhteydessä julkaisen sisäisen blogikirjoituksen aiheesta informaatiovaikuttaminen ja disinformaation tunnistaminen.
4. Kyberturvallisuuskeskuksen tulevaisuuden rekrytoinneissa arvioidaan disinformaation tunnistamisen taitoa lisäämällä haastatteluosuuteen lyhyt testiosuus esimerkkitapauksista.
5. Teen aloitteen Viestintäviraston Viestinnälle siitä, että tulisiko viraston koko henkilökunta perehdyttää informaatiovaikuttamiselle ja disinformaation tunnistamiseen sekä faktantarkistuksen oppeihin osana uuden henkilöstön perehdytysmateriaalia.

7.3 Opinnäytetyön arviointi

Tämän opinnäytetyön tavoitteena oli kuvata mistä disinformaatiossa on kysymys ja miten se tunnistetaan, miten disinformaation tunnistamisen tulisi vaikuttaa Kyberturvallisuuskeskuksen prosesseihin ja miten keskuksen henkilöstö ohjeistaa informaatiovaikuttamisen ja disinformaation varalta. Tämä on samalla ensimmäinen virastossa tehty opinnäytetyö, joka koskee virastossa varsin vähän tunnettua ilmiötä, disinformaatiota. Samalla oli tarkoitus luoda ohjeistus ja malli disinformaation tunnistamiseen. Viiden eri esimerkin avulla olen pyrkinyt konkreettisesti kuvaamaan disinformaatiota leviämistapaa eri median kanavissa, jotta lukija sai konkreettisen tuntuman mahdollisesti manipuloituun, huijaavaan ja tekaistuun sisältöön.

Kyseessä oli työelämän kehittämishanke, jossa tutkittiin tarkkaan rajattua tapausta eli Kyberturvallisuuskeskuksen tilannekuvatuotannon prosessin kehittämistä. Käytin opinnäytetyössäni tutkimusmenetelmänä tapaustutkimusta. Asiantuntijahaastatteluissa nousi toistuvasti esiin samoja keskeisiä teemoja ja kysymyksiä disinformaation leviämisestä. Näiden teemojen kautta pyrin löytämään työpajaan esimerkkejä, joissa tietoa on jollain tapaa vääristelty. Työmenetelmänä käytin työpajaa. Mielestäni tähän asiantuntijatyön kehittämiseen soveltuvat työpajan kaltaiset yhteisölliset menetelmät. Työpajan parhainta antia oli keskustelu, jossa kehitettävää ohjeistusta pystyi yhdessä testaamaan ja tunnistaen vielä tulevaisuuteen jääviä jalostamistarpeita.

Opinnäytetyön kantavaa teemaa disinformaation tunnistamista harjoiteltiin kybertapausten arvioinnilla käyttämällä testimallin kysymyksiä. Testimallin kysymykset syntyivät synteesinä alan kirjallisuutta, haastatteluja ja omaa työelämän kokemusta hyväksi käyttäen.

Tutkimuskysymyksien arvioinneissa nostin esille sen, että disinformaation tunnistamista ei suomalaisessa yhteiskunnassa kansalaisten osalta laajasti tunneta. Informaatiovaikuttaminen ei juurikaan näy monimuotoisessa suomalaisessa mediassa. Suomalainen media tarttuu valtioiden välisiin tapahtumiin, kuten malliesimerkissä MH17 koneen alas ampuminen tai kun on kyse esimerkiksi valtioiden päämiesten tapaamisista ja niiden yhteydessä annetusta varmistamattomasta tiedosta. Toisaalta asiantuntijahaastatteluissa tuli vahvasti ilmi, että meihin vaikutetaan tai mediaa jopa pidetään hallussa erilaisilla ohjatuilla strategisilla narratiiveilla. Haastatteluissa nostettiin myös esille, miten digitaalisten alustojen kautta vääristelty tieto leviää tehokkaasti ja nopeasti.

Euroopan komissio on antanut tiedonannon eurooppalaisesta lähestymistavasta disinformaation torjunnasta verkossa. Se on erityisen huolissaan disinformaatiosta, joka voi aiheuttaa suurta vahinkoa esimerkiksi poliittisessa päätöksenteossa tai menettelyissä. Väärän tiedon leviäminen tunnistetaan tiedonannossa yhdeksi nykyajan suurimmaksi trendiksi. Haastateltavien näkemykset ja Euroopan komission tiedonannon sisällöt ovat jossain määrin ristiriitaisia niihin keskusteluihin nähden joita Suomessa käydään. Tähän voikin todeta, että joko suomalaisessa mediassa ei tunnisteta riittävällä tasolla informaatiovaikuttamista tai disinformaation leviämistä tai sitten sitä esiintyy Suomessa vähemmän kuin muualla.

Sen sijaan kansalaiset altistuvat yhä enemmän profilointiin käyttäessään erilaisia verkkoalustoja ja palveluita. Sosiaalisen median arkipäivää ovat erilaiset botit, väärennetyt identiteetit sekä huijaukset. Tulevaisuuden tiedonvälityksen trendit, erilaisten informaatioalustojen synty, sovellusten ja palveluiden kehittyminen tulee koskemaan myös disinformaation

leviämistä. Nämä molemmat kehityspolut tulivat vahvasti esille haastatteluissa, työpajan keskusteluissa ja Euroopan komission tiedonannossa.

Tulevaisuuden osalta vaikuttaisi siltä, että elämme murrosta. Toisaalta Euroopan komissio ajaa kaikin tavoin tiedon läpinäkyvyyttä, monimuotoisuutta ja uskottavuutta. Halutaan, että disinformaation tunnistamiseen syntyisi kansalaisten käyttöön erilaisia työkaluja ja indikaattoreita tiedon uskottavuuden arvioimiseksi. Verkkopalveluiden algoritmien käyttöön halutaan läpinäkyvyyttä ja tietoa siitä, miten meidän henkilökohtaisia tietojamme käytetään, esimerkiksi mainosten luomiseksi. Toisaalta uskotaan, että suljettujen ekosysteemien määrä kasvaa tulevaisuudessa. Erityisesti tämä koskee tässä vaiheessa WhatsApp-sovellusta, joka on käytetyin tiedonvaihtoon perustuva alusta. Murroksen ylimenokauteen näyttäisi vaikuttavan enemmän kuluttajakäyttäytyminen kuin teknologian antamat eri mahdollisuudet.

Teknologialle on mahdollista antaa tulevaisuudessa suurempi rooli. Keinoälyn käyttö tulee vääjäämättömästi parantamaan hakukoneiden tehokkuutta, vääristellyn tiedon alkuperää tai kykyä verrata eri materiaaleja keskenään. Keinoäly saattaa myös ratkaista nykypäivän disinformaation jakamiseen käytettyjen eri teknologioiden keskinäisriippuvuudet. Tämä tarkoittaa sitä, että voisimme keinoälyn avulla muodostaa tarkempaa kokonaiskuvaa ja jäljittää tiedon alkuperän tehokkaammin.

Opinnäytetyöni kehitti työelämän prosesseja, työelämän taitoja ja faktantarkistuksen tunnettavuutta Viestintävirastossa. Edelliseen lukuun 7.2 on kerätty viisi kehittämiskohdetta Viestintävirastossa, joista neljä ensimmäistä on helposti toteutettavissa. Arvioin, että työni lisää erityisesti tilannekuvatuotteiden laatua ja sen jälkeen, kun materiaali saadaan jakoon sisäisessä intranetissä, se kasvattaa henkilöstön taitoja ja ymmärrystä ilmiöstä laajemmin koko virastossa.

7.4 Oman oppimisen ja opinnäytetyön luotettavuuden arviointi

Oman oppimisen kannalta erityisen hedelmällistä opinnäytetyön laatimisessa on ollut oman ammattitaidon ja oman ymmärryksen lisääminen käsitellyistä aihealueista. Aihealue on ollut oman mukavuusalueeni, kyberturvallisuuden, ulkopuolella ja siitä huolimatta olen jaksanut perehtyä aiheen satoihin materiaalisivuihin. Tapaustutkimus työpajoineen oli hyvä valinta opinnäytetyöhön ja se on antanut uskoa siihen, että myös informaatiovaikuttamisen ja disinformaation tunnistamista voi opetella, ohjeistaa ja myös kouluttaa.

Jos tekisin jotain toisin, en asettaisi itselleni näin tiukkoja aikatauluja kuin nyt olen tehnyt työelämän ohella. Asettamani tiukat aikarajat ovat osin heijastuneet opinnäytetyön laatuun. Toisaalta asettamani aikataulu on kannustanut opinnäytetyön määrätietoiseen eteenpäin viemiseen.

Opinnäytetyöni tutkimusmenetelmänä oli tapaustutkimus ja siihen voidaan soveltaa monenlaisia metodeja. Esimerkiksi aineiston keruussa kaikki menetelmät testaamisesta haastatteluun ovat mahdollisia (Merriam 1998, 28). Merriamin (1998, 134) mukaan myös laadullisissa tapaustutkimuksissa voidaan yleisesti käyttää monia aineiston keruumenetelmiä. Oman opinnäytetyöni tutkimusaineisto koostuu dokumenteista, haastatteluista ja työpajan havainnoista.

Opinnäytetyön tutkimuksen luotettavuus on keskeinen osa työn lopputuloksen arviointia. Tälle opinnäytetyölle asetettiin tavoitteita, joihin on pyritty vastaamaan tapaustutkimuksella. Arvioinnin keskeisiä käsitteitä ovat pätevyys (validiteetti) ja luotettavuus (reliabiliteetti). Pätevyys ja luotettavuus sopivat hyvin määrälliseen tutkimukseen ja on selvää, ettei tapaustutkimuksen luotettavuutta voida arvioida aivan samalla tavalla kuin määrällisen tutkimuksen. Luotettavuuden arvioinnin osalta voidaan pohtia, onko tutkimus johdonmukainen, tuottavatko haastattelut samantapaisia vastauksia ja ovatko tutkittavat käsitteet olleet riittävän selkeitä haastateltaville ja tutkijalle. (Saaranen-Kauppinen, Puusniekka, Kuula, Rissanen & Karvinen 2009, 24-27.)

Pätevyydessä on kysymys siitä, onko opinnäytetyö tehty perusteellisesti ja ovatko siinä olevat johtopäätökset "oikeita". Kehittämistavoitteiden saavuttamisessa ei tyypillisesti ole yhtä täydellistä oikeaa totuutta. Kehittämistavoitteilla haetaan menettelytapoja ja ohjeistuksia, jotka tarpeen mukaan elävät muuttuvassa arjessa. (Saaranen-Kauppinen ym. 2009, 25-27.)

Opinnäytetyön kaikki haastattelut nauhoitettiin haastateltavien suostumuksella ja nauhoitetut haastattelut purettiin tekstiksi. Työpajan ensihavainnot kirjoitettiin yhdessä työpajan osallistujien kanssa. Näin ollen voidaan ainakin todeta, että dokumentointi on ollut luotettavaa. Sekä haastateltavien esittämät näkemykset, että työpajan havainnot antoivat samantapaisia vastauksia, kuin esimerkiksi Euroopan komission tiedonanto disinformaation torjumiseksi verkossa. Nämä vastaavuudet lisäävät osaltaan opinnäytetyön luotettavuutta. Tutkimuskysymys, miten disinformaation tunnistaminen tulisi kehittää Kyberturvallisuuskeskuksen prosesseja jäi vielä kesken, koska tunnistimme työpajassa kysymyksen sisältävän kaksi eri näkökulmaa. Myös tämä lisää osaltaan opinnäytetyön luotettavuutta ja us-

kottavuutta, koska kaikkia asioita ei pystytty ratkaisemaan ja toisaalta se korostaa disinformaation tutkimisen tarvetta jatkossa yhä kokonaisvaltaisemmin. Opinnäytetyön luotettavuutta olisi lisännyt, jos haastattelut olisi voitu tehdä haastateltavien nimillä ja heidän yhteiskunnallinen asema huomioiden.

Tämän opinnäytetyön tavoitteena on kehittää yhtä Viestintäviraston Kyberturvallisuuskeskuksen prosessia. Työssä esitetyt löydökset kuvaavat nykytilaa ja ne ovat päteviä. Prosessi kehittyy viraston ja keskuksen arjessa tapahtuvan oppimisen ja jatkuvan parantamisen kautta. Tutkittavan asian pätevyys ilmenee paremmin työn tuloksen vakuuttavuutena ja uskottavuutena, sekä sellaisena kuin se on työn tekijälle tutkimustilanteessa ilmennyt.

Jatkotyön aiheeksi soveltuisi tutkimus disinformaation tarkistettavien väitteiden valikoitumisprosessista. Jatkossa tulisi arvioida miten kriteerit valitaan ja miten tutkittava tieto rajataan. Tulevaisuudessa olisi mielenkiintoista seurata miten ilmiö kansainvälisesti kehittyy, ja tuleeko Euroopan komissio velvoittamaan jäsenmaitaan ryhtymään kiireellisiin toimiin informaatiovaikuttamisen ja disinformaation torjumiseksi.

Lähteet

Aaltola, J. & Valli, R. 2007. Ikkunoita tutkimusmetodeihin. Jyväskylä. PS-kustannus.

Anttila, P. 2005. Ilmaisu, teos tekeminen ja tutkiva toiminta. Hamina. AKATIIMI OY.

BBC News 2013. Bots now 'account for 61% of web traffic'. Luettavissa: https://www.bbc.com/news/technology-25346235. Luettu: 2.10.2018

BBC News 2016. Adobe Voco ´Photoshop-for-voice' causes concerns. Luettavissa: https://www.bbc.com/news/technology-37899902. Luettu: 27.10.2018

De Cock Buning, M., Allan, R., Bargaoanu, A., Bechmann, A., Curran, N., Dimitrov, D., Dzsinich, G., Frau-Meigs, D., Fubini, F., Gniffke, K., Goyens, M., Gutierrez Velazquez, R., Jiménez Cruz, C., Leclercq, C., Lemarchand, G., Lundblad, N., MacDonald, R., Mantzarlis, A., Markovski, V., Nielsen, R., Nieri, G., Niklewicz, K., Polák, J., Pollicino, O., Raag, I., Rae, S., Riotta, G., Rozukalne, A., Salo, M., Schwetje, S., Steenfadt, O., Stjärne H., Sundermann, M., Turk, Z., Turner, S., Vaisbrodė, N., Van Wijk, W. & Von Reppert-Bismarck, J. 2018. A multi-dimensional approach to disinformation. European Commission. Luettavissa: https://blog.wanifra.org/sites/default/files/field_blog_entry_file/HLEGReportonFakeNewsandOnlineDisinformation.pdf. Luettu: 3.4.2018.

Euroopan komissio 2018. Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle. Eurooppalainen lähestymistapa disinformaation torjuntaan verkossa. Luettavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52018DC0236&from=FI. Luettu: 1.5.2018.

Faktabaari 2018. Faktantarkistus Suomessa. Oppeja vuoden 2018 presidentinvaaleista. Luettavissa: https://faktabaari.fi/baaripuhetta/faktantarkistus-suomessa-oppeja-vuoden-2018-presidentinvaaleista/. Luettu: 11.11.2018.

Fortune 2018. How Faking Videos Became Easy — And Why That's So Scary. Luettavissa: http://fortune.com/2018/09/11/deep-fakes-obama-video/. Luettu: 19.9.2018.

Fox, C.J. 1983. Information and misinformation: an investigation of the notions of information, misinformation, informing, and misinforming.
Luettavissa: https://www.questia.com/read/9787055/information-and-misinformation-an-investigation-of. Luettu: 17.10.2018.

The Guardian 2017. Facebook's key to building communities divided times: augmented reality. Luetavissa: https://www.theguardian.com/technology/2017/apr/18/facebook-mark-zuckerberg-f8-speech-augmented-reality. Luettu: 28.10.2018.

Hirsjärvi, S. & Hurme, H. 2001. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki. Yliopistopaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 1997: Tutki ja kirjoita. Tampere. Tammer-Paino Oy.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2004: Tutki ja kirjoita. Helsinki. Tammi.

Huoltovarmuuskeskus 2014. Kyberympäristö ja kyberturvallisuus. Luettavissa: https://www.varmuudenvuoksi.fi/aihe/kyber/142/kyberymparisto_ja_kyberturvallisuus. Luettu: 30.11.2018.

Jeangène Vilmer, J.-B., A. Escorcia, A., Guillaume, M., Herrera, J. 2018. Information Manipulation: A Challenge for Our Democracies. Luettavissa: https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf. Luettu: 1.10.2018.

Kaminska, M., Gallacher, J., Kollanyi, B., Yasseri, T. & Howard, P. 2017. Social Media and News Sources during the 2017 UK General Election. Oxford University. Luettavissa: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Social-Media-and-News-Sources-during-the-2017-UK-General-Election.pdf. Luettu: 27.10.2018.

Karlova, N.A. & Fisher, K.E 2013. A sosial diffusion model of misinformation and disinformation for understanding human information behaviour. University of Washington. Luettavissa: http://www.informationr.net/ir/18-1/paper573.html#.W8yqqOgzZPY. Luettu: 18.10.2018.

Kauppalehti 2018. Putin käräytti "Putinin" Twitterissä – taitava valetili keräsi miljoona seuraajaa. Luettavissa: https://www.kauppalehti.fi/uutiset/putin-karaytti-putinin-twitterissa-taitava-valetili-kerasi-miljoona-seuraajaa/d0d1e588-f734-4601-a847-1eae2f3117c7. Luettu: 1.12.2018.

Kielikello 2013. Trolli – rölli, kiuso, härnäkkö?. Luettavissa: https://www.kielikello.fi/-/trolli-rolli-kiuso-harnakko-. Luettu: 14.10.2018.

Kortesuo, K. 12.4.2018. Venäjänkielisten naisbottien invaasio Twitterissä - blokkaa pois. Luettavissa: https://eioototta.fi/venajankielisten-naisbottien-invaasio-twitterissa-blokkaa-pois/. Luettu: 27.10.2018.

Kuluttajatutkimuskeskus 2005. Monenlainen tapaustutkimus. Julkaisuja 4/2005. Luettavissa: https://helda.helsinki.fi/bitstream/handle/10138/152279/Monenlainen_tapaus-tutkimus.pdf. Luettu: 11.3.2018.

Kuula, A. 2006. Tutkimusetiikka: Aineistojen hankinta, käyttö ja säilytys. Tampere. Vastapaino.

Kuutti, H. 2015. Varmistusjournalismin työkäytännöt. Jyväskylä. Jyväskylän yliopisto. Luettavissa: https://jyx.jyu.fi/bitstream/handle/123456789/45701/VARMISTUSJOURNA-LISMIN%20TY%C3%96K%C3%84YT%C3%84NN%C3%96T.pdf?sequence=1. Luettu: 1.10.2018.

Laki sähköisen viestinnän palveluista 7.11.2014/917.

Merriam, S. B. 1998. Qualitative research and case study applications in education. San Francisco: Jossey-Bass Publishers

MSB 2018. Att möta informationspåverkan – Handbok för kommunikatörer. Luettavissa: https://www.msb.se/RibData/Filer/pdf/28692.pdf. Luettu: 1.10.2018.

MTV 2017. Osuuspankki vaatii hakkerilta lähes puolta miljoonaa euroa – 17-vuotias perusteli hyökkäystään testaamisella. Luettavissa: https://www.mtvuutiset.fi/artikkeli/osuus-pankki-vaatii-hakkerilta-lahes-puolta-miljoonaa-euroa-17-vuotias-perusteli-hyokkaystaan-testaamisella/6620090#gs.4r7cMyA. Luettu: 30.11.2018.

NATO StratCom COE. 2018. ROBOTROLLING 2/2018. Luettavissa: https://www.strat-comcoe.org/robotrolling-20182-0. Luettu: 1.10.2018.

Ojasalo, K., Moilanen, T & Ritalahti, J. 2014. Kehittämistyön menetelmät. Helsinki. Sanoma Pro.

Rubin, V. L. 2010. On deception and deception detection: Content analysis of computer-mediated stated beliefs. Proceedings of the American Society for Information Science and

Technology. Luettavissa: https://onlinelibrary.wiley.com/doi/abs/10.1002/meet.14504701124. Luettu: 21.10.2018.

Saaranen-Kauppinen, A., Puusniekka, A., Kuula, A., Rissanen, R. & Karvinen, I. 2009. Menetelmäopetuksen tietovaranto. Tampere: Tampereen yliopisto.

Sanastokeskus 2018. Kyberturvallisuuden sanasto. Luettavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf. Luettu: 20.10.2018.

Silverman, C. Perlman, M. 2018. Verification Handbook. The European Journalism Centre. Luettavissa: https://verificationhandbook.com/downloads/verification.handbook.pdf. Luettu: 30.11.2018

Syrjälä, L. & Numminen, M. 1988. Tapaustutkimus kasvatustieteessä. Oulu. Oulun yliopisto.

Statista 2018. Number of monthly active WeChat users from 2nd quarter 2011 to 2nd quarter 2018. Luettavissa: https://www.statista.com/statistics/255778/number-of-active-wechat-messenger-accounts/. Luettu: 27.10.2018.

Thies, J., Zollhofer, M., Stamminger, M., Theobalt, C. & Nießner, M. 2016. Face2Face: Real-time Face Capture and Reenactment of RGB Videos. Stanford University. Luettavissa: https://web.stanford.edu/~zollhoef/papers/CVPR2016_Face2Face/paper.pdf. Luettu: 28.10.2019

Tivi 2017. Maapallon väestöstä yli puolet käyttää internetiä – sosiaalista mediaa 40 %. Luettavissa: https://www.tekniikkatalous.fi/tekniikka/ict/maapallon-vaestosta-yli-puolet-kayttaa-internetia-sosiaalista-mediaa-40-6667907. Luettu: 2.12.2018.

Tivi 2018. Ärsyttääkö törky ja vihapuheTwitterissä? Näin isket takaisin tavalla joka tuntuu. Alma Talent. Luettavissa: https://www.tivi.fi/Kaikki_uutiset/arsyttaako-torky-ja-vihapuhe-twitterissa-nain-isket-takaisin-tavalla-joka-tuntuu-6736534. Luettu: 26.10.2018.

Tuominen, K. & Savolainen, R. 1997. A social constructionist approach to the study of information use as discursive action. Luettavissa: http://www.webcitation.org/6FI8dQZaK. Luettu: 27.10.2018.

Turvallisuuskomitea 2013. Suomen kyberturvallisuusstrategia. Luettavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf. Luettu: 23.4.2018.

Viestintävirasto 2016 a-b. Viestintäviraston toimialan järjestöt ja muut sidosryhmät. Luettavissa: https://www.viestintavirasto.fi/tilastotjatutkimukset/yleistatoimialatiedosta/jarjestotjamuutsidosryhmat.html. Luettu: 23.4.2018.

Viestintävirasto 2017 a-b. Kyberturvallisuuskeskuksen palvelut. Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus/viestintavirastontietoturvapalvelut.html. Luettu: 23.4.2018.

Viestintävirasto 2018 a-e. Viestintäviraston toimialat. Luettavissa: https://www.viestintavirasto.fi/viestintavirasto/virastonesittelyjatehtavat/toimialat.html. Luettu: 23.4.2018.

Wardle, C. & Derakhshan, H. 2017. Information disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe. Luettavissa: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c. Luettu: 1.5.2018.

Yin, Robert K. 1994: Case study research - design and methods. Newbury Park. Sage Publications.

Yle 2015. Yle Pietarin trollitehtaalla – Näin Venäjän propagandaa rustataan kellon ympäri. Luettavissa: https://yle.fi/uutiset/3-7804386. Luettu: 4.5.2018.

Liitteet

Liite 1. Työpajan esitysmateriaali

Työpajan tarkoitus

1. Informaatiovaikuttamisen ymmärryksen lisääminen
2. Median esimerkkien läpikäyminen ja vertaaminen alustavaan ohjeistukseen
3. Yhteenveto oivalluksista

Tutkimuskysymysten arviointi:

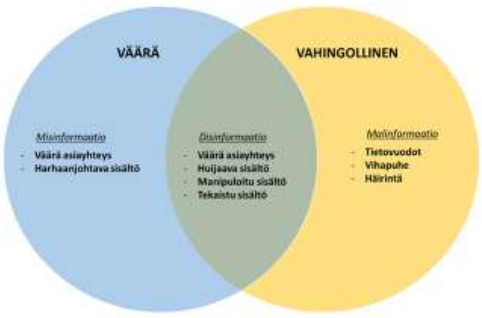
1. Miten informaatiovaikuttaminen tunnistetaan jokapäiväisessä toiminnassa osana Kyberturvallisuuskeskuksen tilannekuvatuotantoa?
2. Miten disinformaation tunnistamisen tulisi vaikuttaa Kyberturvallisuuskeskuksen prosesseihin?
3. Miten Kyberturvallisuuskeskuksen henkilöstö voidaan ohjeistaa informaatiovaikuttamisen varalta

Informaatiovaikuttaminen

- Uhkatekijän muodostavat sellaiset valtiolliset tekijät ja kansalliset ryhmittymät, jotka pyrkivät vaikuttamaan kansallisiin arvokäsitykseen, demokraattiseen päätöksentekoon tai poliittisiin prosesseihin levittämällä vääristeltyä tietoa.
- Vaaleihin vaikuttaminen, päätöksentekoon vaikuttaminen, yleiseen mielipiteeseen vaikuttaminen, epätietoisuuden levittäminen, viranomaisten luottamuksen vähentäminen, ihmisten mieliin vaikuttaminen

Informaation eri lajit

- Misinformaatiolla tarkoitetaan tietoa, joka on väärää, mutta sitä ei ole luotu vahingoittamistarkoituksessa.
- **Disinformaatiolla** tarkoitetaan tietoa, joka on väärää ja harkitusti luotu sekä tarkoituksellisesti julkaistu vahingoittamaan henkilöä, sosiaalista ryhmää tai maata.
- Malinformaatiolla tarkoitetaan tietoa, joka perustuu todellisuuteen ja jonka on ollut tarkoitus pysyä salassa ja julkaisulla on tarkoitus vahingoittaa henkilöä, organisaatiota tai maata.



Disinformaation leviämisen kanavat

- Internetin robotit – botit
- Keskustelevat botit
- Twitterin ja Facebookin puoliautomatisoidut tilit
- Internetin algoritmit
- Organisoitunut yksilö, tahot, trollitehtaat
- Tulevaisuudessa koneoppiminen, virtuaalitodellisuus ja tekoäly ohjaavat tiedon prosessointia ja tietovirtoja.

Nykymalli kybertapausten arviointiin

Nopeaa reagointia vaativat tilanteet:

- Viestintäverkkojen ja -palvelujen häiriöt: Palvelun käyttäminen on häiriintynyt tai estynyt ja käyttäjät havaitsevat ongelman
- Palvelunestohyökkäys: Palvelu ei ole käytettävissä tai on erittäin hidas käyttäjille
- Tietovuoto: Tietomurron kautta saadut tiedot on vuodettu julkisuuteen ja välittömästi hyödynnettävissä
- Haittaohjelma: Haittaohjelma leviää verkkosivuston tai sähköpostin kautta.
- Huijaukset: Phishing- tai muu esim. sähköpostitse tai tekstiviestein leviävä huijaus-kampanja.

Faktantarkistuksen oppeja 2018:

1. Tarkistettavien väitteiden valikoitumisprosessia tulee kehittää: Selkeät kriteerit väitteiden valintaan ja rajaamiseen.
2. Laatu on tärkeämpää kuin määrä. Kaikki esitettyjä väitteitä ei tarvitse tarkistaa.
3. Lähteiden käyttöön ja seikkaperäiseen merkitsemiseen on syytä panostaa.
4. Väitteiden tarkastelussa on tärkeää tuoda esiin niiden sisällöllinen asiayhteys laajemmassa keskustelussa.
5. Faktantarkistusprosessin kansainvälisten kriteereiden seuraaminen ja niiden tekeminen avoimeksi.
6. Tutkijoiden ja toimittajien yhteistyön kehittäminen. Yhtenä keskeisenä askeleena on yhdenmukaistaa ja kehittää asiantuntijoiden löytämistä helpottavia palveluita.
7. Resursseihin panostaminen.

- Lähde: Faktabaari

Testimalli kybertapausten arviointiin

1. Ole terveen epäluuloinen
2. Tarkista julkaisija
3. Tarkista toimittajien nimet ja toimituksen osoitetiedot (oikeita vai keksittyjä), google ja erilaiset rekisterit ovat tähän varsin hyvä väline
4. Tärkeää on lukea koko juttu ei pelkkää otsikkoa ja ingressiä (sisällön tulisi vastata otsikkoa)
5. Tarkista jutun lähteet
6. Tarkista mahdolliset puhutut lainaukset
7. Mikäli jutussa mainitaan tutkimus, tarkista onko tutkimusta olemassa
8. Mahdollisten numeeristen tietojen tarkistus
9. Tarkista uutisen kielioppi ja sävy (herjaukset, jonkun henkilön tikkuun nostaminen jne.)
10. Onko uutinen oikeasti ajankohtainen vai onko sen tarkoitus "kaivella" vanhoja
11. Tarkista sivuston osoitteen oikeellisuus (valesivustot jäljittelevät tunnettuja osoitteita)
12. Vievätkö julkaisun linkit "oikeille" sivustoille

Case1: Malesialaisen MH17 koneen alas ampuminen

BBC:n dokumentti väittää:
Ukrainalaishävittäjä ampui MH17:n alas

Case1: Malesialaisen MH17 koneen alas ampuminen

UUTISET

Uutiset | Ulkomaan uutiset

BBC tyrmää väitteet MH17-dokumentista - Ukrainalainen hävittäjä ei voinut pudottaa matkustajakonetta

25.04.2016 klo 16:43 (muokattu 25.04.2016 klo 16:43)

Kremlille myötämielisten medioiden mukaan BBC:n tuleva dokumentti vahvistaa, että ukrainalainen hävittäjä ampui alas MH17-koneen. BBC kiistää tämän.

Case2: Imatran ampumistapaus

Case3: Iäkkäät miehet karkasivat vanhainkodista

RADIO nova

ETUSIVU UUTISET OHJELMAT MUSIIKKI KILPAILUT KANAVA

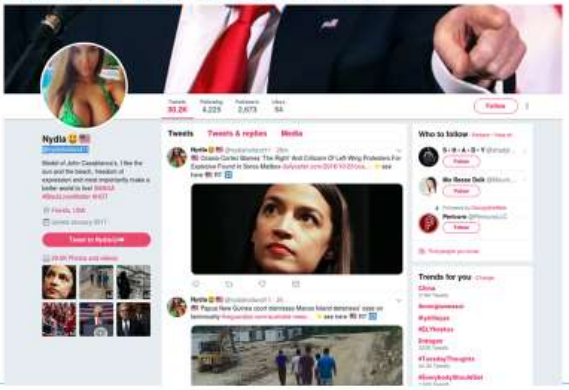
ILMIÖT

läkkäät miehet karkasivat vanhainkodista - poliisi löysi parivaljakon metallifestareilta

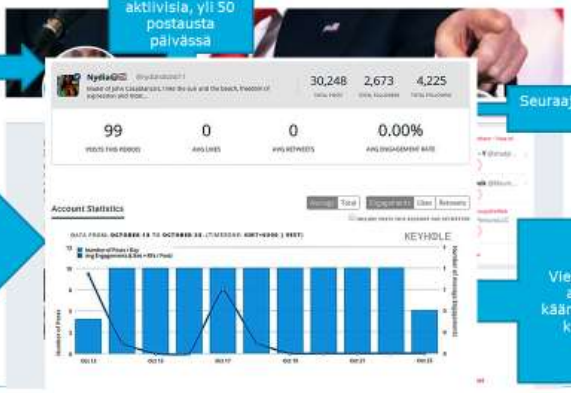
Case4: Suomen rautatieinfran myyminen Norjaan

Ministeri Berner: Suomi pyrkii vähentämään merenkulun päästöjä – myy Suomen rautatieinfran Norjaan

Case5: Bottitilin tunnistaminen



Case5: Bottitilin tunnistaminen



Oivalluksia ja palaute 1/3

- Informaatiovaikuttaminen ei ole jokapäiväisessä tekemisessä läsnä, tarvitaan hoksaamista ja hereillä oloa
- Tilannekuvatuotteiden laatu, luotettavuuden tarkistus on tärkeämpää kuin määrä – viranomaisen uskottavuutta ja luottamusta toimijoihin ei saa menettää
- Lähteiden alkuperä tunnistaminen on keskeistä
- Tunnistettava mihin isoon kokonaisuuteen tapahtumat liittyvät tai ymmärrys siitä yritetäänkö vaikuttaa mielipiteeseen (tarina peittyy helposti vääristeltyjen faktojen joukkoon)
- Uutisoinnin kuvien alkuperän etsiminen uutta ajattelua

Oivalluksia ja palaute 2/3

- Miten erotan uutisoinnin jota on syytä epäillä, mitkä asiat herättävät epäilyn? Lähde, ajankohta, kuvat, linkit?
- Miten tunnistaa vahingossa liikkeelle lähtenyt väärä tieto tarkoituksellisesta?
- Numeeristen faktojen tarkastus helppoa
- Faktantarkistuksen ja faktabaarin käytön lisääminen koetaan tärkeäksi
- Sosiaalisen median sisältöihin ei nykyään juurikaan puututa, pitäisikö?
- Bottitilien vaikuttavuus viranomaisiin arviointiin?

Oivalluksia ja palaute 3/3

- Ohjeistuksen käyttöönotto 2019
- Esimerkkitapausten yhdessä läpikäyminen ja yhdessä oppiminen
- Disinformaation tunnistamiseen erikoistuneen tiimin perustaminen
- Mahdollinen disinformaation oma-aloitteinen etsiminen (resurssien mukaan) ja tuotteistaminen (esim. viikon väärät uutisoinnit ja valetilien paljastaminen) ymmärryksen lisäämiseksi

Deepfake

https://www.youtube.com/watch?v=cQ54GDm1eL0

Viestintävirasto

www.viestintävirasto.fi