Ilari Kilkki

DISINFORMAATION MUODOSTAMAT KYBERUHAT

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Kilkki, Ilari
Disinformaation muodostamat kyberuhat
Jyväskylä: Jyväskylän yliopisto, 2021, 24 s.
Tietojärjestelmätiede, Kandidaatin tutkielma
Ohjaaja: Räisänen, Jaana

Verkottunut informaatioyhteiskunta altistaa jäsenensä jatkuvalle informaatiotulvalle. Informaation seassa on myös tarkoituksellisesti levitettävää, virheellistä informaatiota, jota kutsutaan disinformaatioksi. Disinformaatio leviää kybermaailmassa yhtenä informaatiosodankäynnin välineenä, muodostaen kyberuhkia. Päätöksenteko virheellisen informaation pohjalta voi aiheuttaa merkittävää haittaa niin yksilölle kuin organisaatiollekin. Disinformaatio muodostaa kyberuhan yhteiskunnille heikentämällä kansalaisten luottamusta yhteiskuntien toimintakykyyn ja luotettavuuteen. Tämä tutkielma osoittaa, kuinka myös informaatiosodankäynnin ulkopuolella leviävä disinformaatio muodostaa piileviä kyberuhkia, ja kuinka niiltä voidaan puolustautua. Tehokkain tapa disinformaation aiheuttamien kyberuhkien ennaltaehkäisemiseen on disinformaation tunnistamisen ja siihen reagoimisen opettaminen kansalaisille. Teknologian kehittyminen tarjoaa tehokkaita tapoja disinformaation kohdennettuun levittämiseen tekoälyyn pohjautuvien sovellusten avulla. Vastaavasti disinformaatiota levittävät tahot kyetään tunnistamaan aiempaa tehokkaammin tiedustelussa käytettävien teknologioiden kehittyessä. Tutkielma on toteutettu integroivana kirjallisuuskatsauksena. 23 lähdeaineistona käytetyistä tutkimuksista on etsitty ProQuest Central, SCOPUS ja Google Scholar -tietokannoista, ja julkaistu Julkaisufoorumin luotettaviksi luokittelemissa julkaisuissa.

Asiasanat: disinformaatio, informaatiosodankäynti, kyberuhka,
kyberturvallisuus

ABSTRACT

Kilkki, Ilari
The cyber threats posed by disinformation
Jyväskylä: University of Jyväskylä, 2021, 24 pp.
Information Systems, Bachelor's thesis
Supervisor: Räisänen, Jaana

A networked information society predisposes its members to a continuous flood of information. Some of that information is false and being spread intentionally. That kind of information is called disinformation. Disinformation spreads in the cyber world as one of the instruments of information warfare, thus forming cyber threats. Decision making that is based on false information may cause significant damage to an individual or an organization. Disinformation poses a substantial cyber threat to governments because of how it weakens the citizens' trust to their trustworthiness and ability to function. This study reviews how the disinformation that is being spread outside of information warfare is also causing hidden cyber threats, and how to defend against them. The most effective way to prevent the threats posed by disinformation is teaching the citizens how to recognize disinformation and how to react to it. The advancing technologies offer more effective ways to spread disinformation targetedly with AI-based programs. Respectively the improving intelligence applications are able to identify the spreaders of disinformation more effectively than before. This thesis has been implemented as an integrating literature review. The source material of this study has been collected from ProQuest Central, SCOPUS and Google Scholar databases. 23 scientific articles of the source material have been published in publications which have been defined trustworthy by Julkaisufoorumi.

Keywords: disinformation, information warfare, cyber threat, cyber security

SISÄLLYS

1 JOHDANTO

Tarkoituksellisesti levitettävältä virheelliseltä informaatiolta ei kykene välttymään nykyaikaisessa informaatioyhteiskunnassa. Tällaista informaatiota kutsutaan disinformaatioksi, ja sen omaksuminen osaksi maailmankuvaansa voi aiheuttaa yksilölle merkittävää taloudellista tai fysiologista haittaa, jos kyseessä ovat esimerkiksi sijoitusneuvot tai lääketieteelliset suositukset. (Fallis, 2015). Haitat voivat ilmetä myös yhteiskunnan tasolla, jos kansalaiset menettävät luottamustaan viranomaisiin, hallitukseen ja demokratiaan haitallisen disinformaation vaikutuksesta. Yhteiskunnan sisäisen luottamuksen heikentäminen toimiikin motiivina useiden informaatiosodankäynnissä hyödynnettävien informaatio-operaatioiden taustalla. Haitallista disinformaatiota levittävät informaatio-operaatiot tapahtuvat kybermaailmassa, muodostaen kyberuhkia. (Clapper, Lettre & Rogers, 2017).

Järjestelmällisesti levitettävä disinformaatio ei kuitenkaan rajoitu vain organisoituihin informaatio-operaatioihin. Poliittiset organisaatiot, viranomaiset ja yritykset käyttävät disinformaatioksi luokiteltavia viestintäkeinoja viestiessään kohdeyleisöilleen. (Edwards, 2021). Tarkoituksellisen harhaanjohtava ja valheellinen viestintä voi heikentää yhteiskunnan sisäistä luottamusta, vaikka ei siihen lähtökohtaisesti pyrkisikään (Kavanagh & Rich, 2018, s. 36, 62).

Tämä tutkielma selvittää, miksi myös informaatiosodankäynnin ulkopuoliseen disinformaatioon tulisi suhtautua potentiaalisena kyberuhkana. Aihealuetta ei ole tiettävästi tutkittu kyberturvallisuuden näkökulmasta aikaisemmin.

Kyberturvallisuutta uhkaavan disinformaation määritelmän laajentamisen lisäksi tämä tutkielma selvittää Suomen valmiutta haitallisen disinformaation aiheuttamien kyberuhkien ennaltaehkäisemiseen ja niihin reagoimiseen. Tämä tutkielma argumentoi, että keskeinen puolustusvalmiutta heikentävä ongelma on disinformaation tunnistamisen vaikeus.

Tämä tutkielma on toteutettu integroivana kirjallisuuskatsauksena, joka syventyy disinformaation muodostamiin uhkiin kyberturvallisuuden näkökulmasta. Kyberuhkia käsitellään sekä yksilön että yhteiskunnan tasolla. Synteesiä muodostuu tutkielman kannalta keskeisiä käsitteitä määriteltäessä, kun aiem-

pien tutkimusten määritelmiä ja niihin pohjautuvia johtopäätöksiä sulautetaan yhteen.

Tutkielma vastaa tutkimuskysymyksiin ”Millä perusteilla myös informaatiosodankäynnin ulkopuolinen disinformaatio saattaa muodostaa piileviä kyberuhkia?” ja ”Kuinka yksilöt ja yhteiskunnat kykenevät puolustautumaan disinformaation muodostamilta kyberuhilta?”

23 tutkielman lähdeaineistona käytetyistä tutkimuksista on etsitty ProQuest Central, SCOPUS ja Google Scholar -tietokannoista, ja julkaistu Julkaisufoorumin luotettaviksi luokittelemissa julkaisuissa.

Clapperin, Lettren ja Rogersin (2017) julkaisema selonteko Foreign Cyber Threats to the United States on laadittu Yhdysvaltojen puolustusministeriön pyynnöstä. Rogers on toiminut Yhdysvaltojen kyberturvallisuudesta vastaavan viraston (United States Cyber Command) varajohtajana. Näiden seikkojen pohjalta selonteossa esitettyjä kyberuhkien määritelmiä on pidettävä luotettavina, vaikka artikkelia ei olekaan julkaistu Julkaisufoorumin luotettavaksi luokittelemassa julkaisussa.

Edward Bernaysin kommentit tiedotus- ja suhdetoiminnasta ja propagandasta on videoitu Adam Curtisin vuoden 2002 dokumenttielokuvaan A Century of the Self, joka voitti muun muassa History Today -julkaisun palkinnon Historical Film Of The Year. History Today on Julkaisufoorumin luotettavaksi luokittelema julkaisu.

Ensimmäisessä sisältökappaleessa määritellään disinformaation käsite, ja perustellaan miksi myös informaatiosodankäynnin ulkopuolinen disinformaatio voi aiheuttaa vakavaa haittaa. Toisessa kappaleessa määritellään kyberturvallisuuden, kyberuhan ja informaatiosodankäynnin käsitteet. Lisäksi käydään läpi millaisia kyberuhkia informaatiosodankäynti aiheuttaa, ja perustellaan miksi myös informaatiosodankäynnin ulkopuolinen disinformaatio voi muodostaa yhteiskunnan toimintaa haittaavan kyberuhan. Kyberuhkia käsitellään sekä yksilön että yhteiskunnan näkökulmasta. Viimeisessä kappaleessa käydään läpi Suomen nykyistä puolustusvalmiutta disinformaation muodostamia kyberuhkia vastaan. Tarkastellaan myös kehittyvien teknologioiden lähitulevaisuudessa muodostamia uhkakuvia ja mahdollisuuksia kyberturvallisuuden näkökulmasta.

2 DISINFORMAATIO

Tässä kappaleessa avataan disinformaation määritelmä synteesiä muodostaen, ja kerrotaan millä tavoin disinformaatio leviää kybermaailmassa. Lopuksi perustellaan, miksi tiedotus- ja suhdetoiminnalle tyypilliseen tarkoituksellisen harhaanjohtavaan viestintään tulisi suhtautua potentiaalisesti haitallisena disinformaationa.

2.1 Määritelmä ja leviämistavat kyberavaruudessa

Disinformaatio on virheellistä informaatiota, jonka erottaa misinformaatiosta sen virheellisyyden tahallisuus. Disinformaatioksi lasketaan esimerkiksi harhaanjohtava mainostaminen niin yritysten kuin poliitikkojenkin toimesta, hallituksen julkaisema propaganda, muokatut valokuvat, internetissä leviävät petokset ja manipuloidut Wikipedia-artikkelit. (Fallis, 2015).

Faktapohjainen informaatio pyrkii tarkoituksellisesti lisäämään vastaanottajiensa tietoisuutta, näkökulmia ja ymmärrystä käsittelemistään asioista. Disinformaatio koostuu tarkoituksellisesta väärentelystä, harhaanjohtamisesta ja teeskentelystä. (Innes, 2020).

Viestinnän tutkimuksen sisäisen konsensuksen mukaan disinformaatio itsessään on arvoneutraalia. Disinformaatiopohjaiseen viestintään suhtaudutaan yhtenä viestinnän välineenä. (Cunningham, 1992). Bernaysin (1942) mukaan disinformaatiopohjaista viestintää kyetään käyttämään myös eettisesti kestävien tavoitteiden saavuttamiseen.

Fallisin (2015) ja Innesin (2020) määritelmille yhteistä on disinformaation tahallinen pyrkimys harhaanjohtamiseen. Tahallisuus implikoi, että disinformaation alkuperäisellä laatijalla on ollut motiivi sen laatimiselle. Näiden havaintojen pohjalta disinformaatio kyetään määrittelemään virheelliseksi informaatioksi, joka pyrkii tahallisesti johtamaan kohdeyleisöään harhaan, ja jonka alkuperäisellä laatijalla on motiivi harhaanjohtamiselle. Tällaiseen informaatioon pohjautuvan viestinnän haitallisuutta tai hyödyllisyyttä kyetään arvioi-

maan vain viestinnän tosiasiallisia vaikutuksia mittaamalla, koska itse disinformaatio on arvoneutraalia.

Disinformaation määritelmän laajuuden johdosta lienee perusteltua todeta, ettei siltä kykene välttymään nykyaikaisessa informaatioyhteiskunnassa. Kuka tahansa voi julkaista sosiaaliseen mediaan ja internetin keskustelupalstoille uutta informaatiota, jonka todenperäisyyttä ei useinkaan tarvitse perustella. Tästä syystä moni sosiaalisen median ja keskustelupalstojen käyttäjä altistuu päivittäin suurelle määrälle informaatiota, jonka todenperäisyydestä hänellä ei ole varmuutta. Tämä saattaa johtaa myös tilanteeseen, jossa alustojen käyttäjät luottavat hyväuskoisesti tuttujensa jakamaan disinformaatioon, ja mahdollisesti jakavat sitä eteenpäin.

Yksittäisten ihmisten sosiaaliseen mediaan ja keskustelupalstoille jakamien julkaisujen lisäksi disinformaatio kykenee leviämään internetissä samojen mekanismien avulla kuin kohdennetut mainoksetkin. Esimerkiksi valheellisia uutisia kyetään levittämään kohdennetusti internet-palveluiden käyttäjistä kerättyjen tietojen avulla. (Bradshaw, 2019). Tämä on mahdollista, koska monet verkkosivut rahoittavat ylläpitoaan vuokraamalla sivuillaan sijaitsevia mainospaikkoja, joissa kolmannet osapuolet kykenevät julkaisemaan sivun käyttäjille kohdennettuja mainoksia (Hughes & Waismel-Manor, 2021). Mainonnan kohdentaminen perustuu käyttäjän aiemmasta internet-toiminnasta kerättyjen tietojen automaattiseen analysointiin. Esimerkiksi tietystä vaaliehdokkaasta tietoa etsinyt henkilö voi törmätä verkkosivulla mainoksiin, jotka johtavat valeuutissivustoille. Valeuutissivustoilla julkaistavat valeuutiset saattavat esittää ehdokkaan joko harhaanjohtavan positiivisessa tai negatiivisessa valossa. (Hughes & Waismel-Manor, 2021; Bradshaw, 2019). Valeuutisia julkaisevien verkkosivustojen liiketoimintalogiikka perustuu sivuston kävijämäärän maksimoimiseen. Valheelliset ja tunteisiin vetoavat väittämät herättävät kävijöiden mielenkiinnon, ja saavat heidät jakamaan artikkelin linkkiä. Yritysten voitot mainostilan vuokraamisesta kasvavat yhdessä internetjulkisuuden kanssa. (Edwards, 2021). Toinen motiivi tällaisten valeuutisten julkaisemiselle on pyrkimys vaikuttaa ihmisten mielikuviin ehdokkaista, ja tätä kautta myös lopulliseen äänestystulokseen (Lei, 2019).

2.2 Disinformaation hyödyntäminen tiedotus- ja suhdetoiminnassa

Disinformaatio ei rajoitu pelkästään informaatiosodankäynnin seurauksena leviäviin valeuutisiin. Tiedotus- ja suhdetoimintaa (engl. Public Relations) toiminnassaan hyödyntävät organisaatiot ovat vastuussa merkittävästä osasta mediassa ja kybermaailmassa leviävästä disinformaatiosta. Järjestelmällinen valehteleminen ja harhaanjohtaminen ovat olleet keskeisiä viestinnän keinoja politiikassa jo ensimmäisestä maailmansodasta saakka (Edwards, 2021).

Verčič, van Ruler, Bütschi ja Flodin (2001) tiivistävät tiedotus- ja suhdetoiminnan koostuvan kaikista organisaation toimista, joilla se pyrkii vaikuttamaan ihmisten mielipiteisiin itsestään ja toimistaan. Kyseisiin toimiin lukeutuvat muun muassa maineenhallintaan tähtäävä viestintä ja mainonta.

Fallis (2015) määrittelee harhaanjohtavan mainonnan disinformaatioksi. Harhaanjohtavan mainonnan taustalla on selkeä motiivi muodostaa todellisuutta positiivisempia mielikuvia mainostetuista tuotteista. Kansainvälisessä markkinoinnin tutkimuksessa on havaittu, että kuluttajat ostavat enemmän sellaisia tuotteita, joista heille on muodostunut positiivinen mielikuva mainonnan perusteella (Ryu, L'Espoir Decosta & Andéhn, 2016). Disinformaatiopainotteinen mainonta toimii yhtenä liiketoiminnan tehostamisen välineistä, joita hyödyntämällä yritykset pyrkivät maksimoimaan liikevoittonsa.

Tiedotus- ja suhdetoimintaan pohjautuvassa viestinnässä on normaalia pysyä vaiti aihealueista, joista viestimisen koettaisiin aiheuttavan organisaatiolle mainehaittaa. Mikäli organisaation edustajalta kysytään tällaisesta aiheesta, hän pyrkii usein muodostamaan siitä todellisuutta positiivisemman mielikuvan viestinnän kohdeyleisölle. (Edwards, 2021). Toisinaan turvaudutaan myös suoranaiseen valehteluun mainehaittojen välttämiseksi, kuten esimerkiksi Watergate-skandaalissa (Kavanagh & Rich, 2018, s. 62). Tarkoituksellisen harhaanjohtava informaatio lasketaan sekä Ennisin (2020) että Fallisin (2015) määritelmillä disinformaatioksi.

Tiedotus- ja suhdetoiminnan tieteenalan perustanut Edward Bernays (1942) suhtautui disinformaatioon yhtenä monista viestinnän välineistä, joita hyödyntämällä mielipiteitä kyetään muokkaamaan tavoitteiden kannalta suotuisimmiksi. Bernays tuli tunnetuksi vastattuaan propagandaoperaatiosta, jonka ansiosta Yhdysvaltojen väestö antoi laajan hyväksyntänsä toiseen maailmansotaan liittymiselle. Bernays myönsi ennen kuolemaansa, että Public Relations oli tosiasiassa uusi, vähemmän negatiivisesti latautunut termi propagandalle. Uuden nimen suojissa kyettiin tutkimaan sotapropagandassa käytettyjen viestintätekniikoiden soveltuvuutta rauhan ajan politiikkaan ja liiketoimintaan. (Curtis, 2002). Cunninghamin (1992) mukaan propaganda viittaa viestintään, jonka avulla pyritään muuttamaan kohdeyleisön käyttäytymistä.

Myös tiedotus- ja suhdetoiminnan oheistuotteena leviävän disinformaation hyödyllisyyttä tai haitallisuutta kyetään arvioimaan vain sen tosiasiallisia vaikutuksia mittaamalla. Vaikka maineenhallinnan motiivina onkin suojella viestijää mainehaitoilta, saattaa viestintä aiheuttaa yhteiskunnan laajuista haittaa. Kavanagh ja Rich (2018, s. 36) toteavat, että harhaanjohtava ja valheellinen viestintä viranomaisten ja poliitikkojen toimesta heikentää yhteiskunnan sisäistä luottamusta hallitukseen ja demokratiaan.

3 DISINFORMAATION MUODOSTAMAT KYBERUHAT

Tässä kappaleessa määritellään kyberturvallisuuden, kyberuhan ja informaatiosodankäynnin käsitteet. Käydään myös läpi millaisia kyberuhkia informaatiosodankäynnin operaatioista peräisin oleva disinformaatio aiheuttaa. Lopuksi tarkastellaan kuinka informaatiosodankäynnin ulkopuolinen disinformaatio muodostaa piileviä kyberuhkia. Sekä informaatiosodankäynnin sisä- että ulkopuolisia kyberuhkia käsitellään niin yksilön kuin yhteiskunnankin näkökulmasta.

3.1 Kyberturvallisuuden ja kyberuhan määritelmät

Termi kyberturvallisuus on esiintynyt mediassa säännöllisesti jo yli vuosikymmenen, mutta sillä ei ole vieläkään yksiselitteistä ja globaalisti hyväksyttyä määritelmää (Schatz, Bashroush & Wall, 2017). Schatz ym. (2017) määrittelevät kyberturvallisuuden koostuvan lähestymistavasta ja toimista, joita organisaatiot ja valtiot noudattavat kyberavaruudessa käytettävien tietojen ja omaisuuden luottamuksellisuuden, eheyden ja saatavuuden suojaamiseksi.

Konkreettisemman määritelmän tarjoaa Sales (2013), jonka mukaan kyberturvallisuus koostuu toimista, joilla pyritään turvaamaan yhteiskunnan toiminnan kannalta kriittisen infrastruktuurin kestävyys ja turvallisuus. Kriittiseksi infrastruktuuriksi lasketaan esimerkiksi telekommunikaatio-, tiedonsiirto- ja sähköverkostot.

Kyberuhaksi määritellään kybermaailmassa tapahtuva toiminta, joka kykenee aiheuttamaan yhteiskunnallista haittaa. Tällaisia toimia ovat esimerkiksi yhteiskunnan kriittisen infrastruktuurin lamauttaminen ja sisäisen luottamuksen heikentäminen disinformaatiopohjaisella viestinnällä. (Clapper, Lettre & Rogers, 2017). Clapperin, Lettren ja Rogersin (2017) mukaan kyberuhkia ei kyetä koskaan eliminoimaan täysin, koska informaatioteknologia tulee aina sisältämään tietoturva-aukkoja, ja ihmiset tulevat tekemään inhimillisiä virheitä.

Kyberuhan määritelmään tulisi sisällyttää yksilöille tosiasiallista haittaa aiheuttavat uhat, jotka leviävät kyberavaruudessa. Schatz ym. (2017) havaitsivat, että kyberturvallisuuden moninaisille määritelmille on yhteistä niiden organisaatiokeskeisyys. Täten on loogista, että myös kyberuhkia käsitellään organisaatioiden näkökulmasta. Suoranaisesti yksilöiden kyberturvallisuutta käsittelevä akateeminen tutkimus on niin vähäistä, ettei tämän tutkielman lähdeaineistoksi löytynyt yhtäkään tutkimusta aiheesta.

3.2 Informaatiosodankäynnin määritelmä ja siinä hyödynnettävän disinformaation muodostamat kyberuhat

Informaatiosodankäynnin määritteleminen konkreettisesti on haastavaa, koska se eroaa perinteisestä sodankäynnistä merkittävästi. Kybermaailmassa valtioiden väliset rajat hämärtyvät, koska tietoverkot tarjoavat pääsyn kaikkialle maailmaan muutamassa sekunnissa. Virallisia sodanjulistuksia ei käytetä, eikä sotatoimista oteta vastuuta. (Lei, 2019). Informaatiosodankäynnin operaatioiden havaitseminen on erittäin vaikeaa, samoin kuin niiden vaikutuksilta suojautuminen, koska ne keskittyvät suurelta osin monimutkaiseen kybermaailmaan (Lei, 2019).

Lei (2019) määrittelee informaatiosodankäynnin tarkoittavan informaation taktista ja strategista hyödyntämistä edun saavuttamiseksi. Taddeo (2012) tarjoaa laajemman määritelmän, jonka mukaan informaatiosodankäynti on informaatio- ja viestintäteknologioiden hyödyntämistä poliittisen auktoriteetin määrittämän sotilaallisen hyökkäys- tai puolustusstrategian toteuttamiseksi. Toiminta tähtää vihollisen informaatioresurssien välittömään haltuunottoon tai sekasorron aiheuttamiseen niiden keskuudessa (Taddeo, 2012).

On huomioitavaa, että kaikki informaatio- ja viestintäteknologiaa hyödyntäen toteutetut sotilaalliset toimet lasketaan osaksi informaatiosodankäyntiä. Tällaisten toimien avulla pyritään lamauttamaan vihollisen kriittistä infrastruktuuria. Mahdollisesti tunnetuin esimerkki tällaisesta operaatiosta on Iranin ydinvoimaloiden sabotoiminen Stuxnet-viruksen avulla Israelin ja Yhdysvaltojen toimesta. (Taddeo, 2016). Termit informaatiosodankäynti (engl. Information warfare) ja kybersodankäynti (engl. Cyber warfare) ovat laajalti muodostuneet synonyymeiksi englanninkielisessä tutkimuksessa (Taddeo, 2016). Selkeyden vuoksi informaatiosodankäynti tulisi erottaa kybersodankäynnin käsitteestä, koska informaatiosodankäyntiä voi harjoittaa myös kybermaailman ulkopuolella. Tämä tutkielma keskittyy informaatiosodankäynnin operaatioihin, joissa hyödynnetään disinformaation levittämistä kyberavaruudessa.

Informaatiosodankäynti on muuttunut merkittävästi 2010-luvulla. Sosiaalisen median alustat mahdollistavat täysin uudenlaisen tavan saavuttaa sotatoimien päämäärät ampumatta laukaustakaan. Kohdennetun markkinoinnin avulla yksittäisiä ihmisiä kyetään pommittamaan disinformaatiolla, jonka avulla pyritään muuttamaan heidän käyttäytymistään. (Lei, 2019). Disinformaatio

on äärimmäisen voimakas mielipidevaikuttamisen väline, koska ihmiset analysoivat todella pienen osan ympäristöstään omaksumastaan informaatiosta. Muistiin tallentunut disinformaatio voi vaikuttaa ihmisen myöhempiin päätöksentekoprosesseihin alitajuisesti. Tästä syystä informaatiosodankäynti keskittyy yhä enemmän disinformaation levittämiseen. (Arazna, 2015).

Keskeisin disinformaation muodostama kyberuhka on yhteiskunnan sisäisen luottamuksen heikentyminen kansainvälisiin instituutioihin, hallitukseen ja viranomaisiin (Clapper, Lettre & Rogers, 2017). Heidän mukaansa heikentynyt luottamus muodostaa jatkuvasti suuremman riskin yleiselle turvallisuudelle. Kyberuhka konkretisoituu valtoimenaan leviävinä huhuina, propagandana, salaliittoteorioina ja valeuutisina (Innes, 2020). Tarpeeksi monien uskoma valheellinen idea kykenisi aiheuttamaan valtion sisäisen vallankumouksen, koska valheen sisäistäneet ihmiset uskoisivat vakaasti toimivansa hyvän asian puolesta.

Informaatiosodankäynnin yksilöille muodostamia kyberuhkia ei ole tiettävästi käsitelty laajemmin kyberturvallisuuden tutkimuksissa, jotka keskittyvät pääosin organisaatioiden tasolla ilmenevien ongelmien torjuntaan (Schatz ym., 2017). Tulevissa tutkimuksissa tulisi selvittää informaatiosodankäynnin vaikutuksia yksilötasolla, ja kehittää menetelmiä näiden vaikutusten mittaamiseen.

3.3 Informaatiosodankäynnin ulkopuolisen disinformaation muodostamat piilevät kyberuhat

Informaatiosodankäynnin ulkopuolinen disinformaatio pitää sisällään kaiken tarkoituksellisen harhaanjohtamisen, jonka motiivina ei ole sodankäynnillisen edun saavuttaminen. Huijauksiin perustuvat kyberrikokset muodostavat yksilöiden taloutta uhkaavan kyberuhan. Lähivuosien kenties tunnetuin esimerkki on kryptovaluutta OneCoin, jota markkinoitiin globaalisti BitCoinin syrjäyttäjänä. OneCoiniin ehdittiin investoida kymmeniä miljardeja dollareita, ennen kuin paljastui, että kyseessä on ponzi-huijaus. (BBC, 2019). Toisen tunnetun esimerkin muodostavat pääosin intialaiset huijauspuhelukeskukset, joista soitellaan ihmisille ympäri maailman. Huijarit esiintyvät jonkin tunnetun yrityksen, esimerkiksi Microsoftin, työntekijöinä ja pyytävät huijattavaa antamaan heille etäkäyttöyhteyden tietokoneeseensa. Yhteyden muodostuttua he pyrkivät siirtämään huijattavan pankkitilin sisällön omille tileilleen. (Browning, 2020).

Yksilöiden terveydelle haitallisia kyberuhkia muodostavat internetissä leviävät lääketieteelliset neuvot, jotka eivät perustu lääketieteelliseen tutkimukseen vaan juoruihin ja huhuihin. Anti-vaccine liikkeen jäsenet vastustavat kaikkia rokotteita, koska olettavat niiden aiheuttavan haitallisia sivuvaikutuksia, joista niitä testaavat henkilöt on heidän mukaansa lahjottu vaikenemaan. Rokotusvastaisuus on kasvanut maailmanlaajuisesti liikkeen suosion myötä. (Jolley & Douglas, 2014; Kavanagh & Rich, 2018, s. 22-23).

Myös informaatiosodankäynnin ulkopuolinen disinformaatio aiheuttaa yhteiskunnan sisäisen luottamuksen heikentymistä. Edwardsin (2021) mukaan disinformaatiotutkimus osoittaa, ettei voida enää yleistää ihmisten luottavan media-alan yritysten julkaisemiin uutisiin. Faktapohjaisten uutisten oletetaan olevan valheellisia, fiktioon pohjautuviin uutisiin uskotaan totuutena, ja yleistä luotettavuutta arvioidaan väitteiden ja mediayritysten suosion perusteella faktapohjaisuuden sijaan. (Edwards, 2021).

Kavanagh ja Rich (2018) analysoivat kirjassaan Truth Decay yhteiskunnan sisäisen luottamuksen heikentymisestä Yhdysvalloissa. Sivuilla 34 ja 68 esiteltyjen kyselytutkimusten mukaan enää 9 % yhdysvaltalaisista luotti maansa hallitukseen vuonna 2016. Luottamus oli alle 15 % myös Barack Obaman hallintokaudella, ja se on laskenut 1960-luvun puolivälistä saakka, jolloin 78 % vastanneista ilmoitti luottavansa hallitukseen. Yksi luottamuksen mittareista kyselyissä on kansalaisten luottamus hallituksen julkaiseman informaation oikeellisuuteen (s. 68). Kavanagh ja Rich (2018, s. 36) toteavat yhteiskunnallisten instituutioiden, median ja yritysten harjoittaman viestinnän olleen osasyy luottamuksen rappeutumiseen. Luottamusta heikentäväksi toiminnaksi arvioitiin informaation salaaminen (s. 36), sen esittäminen tarkoituksellisesti harhaanjohtavasti ja valehteleminen (s. 62). Esimerkkejä viranomaisten suoranaisesta valehtelusta tarjoavat Watergate-skandaali (Kavanagh & Rich, 2018, s. 62) ja James Clapperin eroaminen Yhdysvaltojen tiedustelupalveluiden ylimmän johtajan tehtävistään hänen valehdeltuaan kongressille, ettei National Security Agency harjoita yhdysvaltalaisten massavakoilua (Ackerman, 2016). Myös lobbaaminen, joka lasketaan osaksi tiedotus- ja viestintätoimintaa, rapauttaa luottamusta poliittisen päätöksenteon demokraattisuuteen. Lobbaamista on kritisoitu sen pyrkimyksestä varmistaa, että poliittiset päätökset tehdään vaikutusvaltaisten yritysten ja organisaatioiden ehdoilla, äänestäjien vaatimukset sivuuttaen. (Edwards, 2021).

Jatkuva ja normalisoitu totuuden kaunistelu ja ikävistä faktoista vaikeneminen vaikuttavat suoraan demokratian toimivuuteen ja uskottavuuteen, koska äänestäjillä ei ole täysin totuuteen perustuvaa kuvaa asioista (Edwards, 2021). Edwardsin (2021) mukaan faktoista vaikeneminen on tulkittavissa disinformaatiopohjaiseksi viestinnäksi, koska niin toimimalla pyritään todellisuutta positiivisempien mielikuvien muodostamiseen. Hän pitää disinformaatioon pohjautuvaa viestintää tiedotus- ja suhdetoiminnan palveluita tarjoavien yritysten elinehtona, koska toisinaan asiakkaiden tarpeisiin on helpointa vastata viestimällä sidosryhmille tarkoituksellisen harhaanjohtavasti.

Mitä enemmän kansan luottamus aiemmin luotettaviksi informaatiolähteiksi luokiteltuihin hallitukseen, televisiouutisiin ja sanomalehtiin heikentyy, sitä todennäköisemmin he etsivät informaatiota uusista lähteistä. Näiden lähteiden luotettavuus on usein kyseenalainen, ja informaation etsiminen niistä saattaa altistaa ihmiset haitalliselle disinformaatiolle. (Kavanagh & Rich, 2018, s. 37). Ilmiö on johtanut vaalikampanjoihin, joissa poliitikot pyrkivät kohottamaan kannatustaan esimerkiksi väittämällä ilmastonmuutosta huijaukseksi havaittuaan suuren määrän äänestäjistä uskoneen niin jo ennestään (s. 39-40).

Tässä kappaleessa mainittujen seikkojen pohjalta on perusteltua todeta myös informaatiosodankäynnin ulkopuolisen disinformaation muodostavan kyberuhkia, niin yksilöille kuin yhteiskunnillekin. Uhat tiedostetaan jo, mutta niihin ei suhtauduta kyberuhkina. Yleistä kyberturvallisuutta kyettäisiin kohentamaan, jos myös tällaisia uhkia korostettaisiin kyberuhista varoittavassa viestinnässä.

4 DISINFORMAATION MUODOSTAMILTA KYBERUHILTA PUOLUSTAUTUMINEN

Tämä kappale tarkastelee jo olemassa olevia tapoja disinformaation muodostamilta kyberuhilta puolustautumiseen, ja kuinka niitä hyödynnetään Suomen kyberturvallisuusstrategiassa. Lisäksi pohditaan nykyisen puolustusvalmiuden heikkouksia, ja kuinka puolustusvalmiutta voitaisiin tehostaa yhteiskunnan tasolla. Lopuksi käsitellään jatkuvasti kehittyvien teknologioiden avaamia mahdollisuuksia disinformaation tehokkaampaan, kohdennettuun levittämiseen. Kehittyvät teknologiat tehostavat vastapainoisesti myös viranomaisten kykyä paikallistaa disinformaatiota levittäviä tahoja, mikä helpottaa niiden toimintaan puuttumista.

4.1 Suomen nykyinen puolustusvalmius disinformaation muodostamia kyberuhkia vastaan

Clapper, Lettre ja Rogers (2017) toteavat, ettei koskaan kyetä saavuttamaan tilannetta, jossa kyberuhat eivät enää uhkaisi yhteiskunnan kriittisiä rakenteita, koska tietotekniikka tulee aina sisältämään tietoturva-aukkoja, ja ihmiset tekevät inhimillisiä virheitä. Tästä pessimistisen realistisesta lausahduksesta huolimatta valtioiden tasolla varaudutaan kyberuhkien torjuntaan. Suomi on linjannut kyberturvallisuuden kohentamiseen tähtääviä toimiaan viralliseen kyberturvallisuusstrategiaansa, jonka uusin versio on julkaistu vuonna 2019. Tämä tutkielma keskittyy vain kyberturvallisuusstrategian osuuksiin, joiden voidaan olettaa viittaavan disinformaation muodostamilta kyberuhilta puolustautumiseen.

Suomen kyberturvallisuusstrategiassa (2019) todetaan: ”Jokainen yksilö on tärkeä kyberturvallisuustoimija, joka omilla arjen kyberturvallisuutta parantavilla teoilla voi vaikuttaa omaan ja muiden kyberturvallisuuteen. Kansallisesti on varmistettava, että jokaisella on riittävät valmiudet toimia turvallisesti digitaalisessa toimintaympäristössä.” ja ”Valtakunnallista digiturvallisuuden kou-

lutus- ja harjoitusjärjestelmää vahvistetaan osana julkisen hallinnon digitaalisen turvallisuuden koulutusta. Sillä kehitetään julkishallinnon, yritysten ja muiden sidosryhmien työntekijöiden sekä kansalaisten osaamista." Lukijalle jää epäselväksi ketä tarkalleen ottaen koulutetaan, minkä tiimoilta, miten ja milloin. Toki kyseessä ovat vain strategiset linjaukset siitä, mitä jonkun tulisi joskus tehdä. Se, kuka tai ketkä näitä linjauksia tulevat toteuttamaan, jää epäselväksi.

Disinformaation muodostamien kyberuhkien torjumisessa on keskeistä kyetä tunnistamaan haitallinen disinformaatio. Disinformaation muodostamat haitat konkretisoituvat vain, jos disinformaatio pääsee vaikuttamaan ihmisten käyttäytymiseen. Näin ei pääse käymään, jos ihminen ymmärtää motiivit disinformaatiopohjaisen viestinnän taustalla, ja osaa jättää disinformaation omaan arvoonsa, ja varoittaa muita luottamasta tällaiseen viestintään. Näin ollen ihmisten valistaminen aihealueen tiimoilta on tehokkain vastatoimi disinformaation muodostamia uhkia vastaan (Benzel, 2021). Suomen kyberturvallisuusstrategia (2019) mainitsee ihmisten kouluttamisen kyberturvallisuuden tiimoilta kahteen otteeseen, mutta ei täsmennä sisältäisikö koulutus haitallisen disinformaation tunnistamiseen ja siihen reagoimiseen valmistavaa sisältöä. Yhdysvalloissa koulutetaan ihmisiä aktiivisesti kyberturvallisuudesta, mutta koulutus keskittyy yritysten henkilöstöön ja korkeakouluopiskelijoihin – myös he painottavat organisaatiotason puolustautumista yksilötason sijaan (Mcduffie & Piotrowski, 2014).

Toinen tapa esimerkiksi valeuutisilta suojautumiseen olisi internetin palveluntarjoajien asettaminen vastuuseen heidän palveluissaan julkaistavasta disinformaatiopohjaisesta sisällöstä. Tämä onnistuisi lainsäädännöllisten toimenpiteiden avulla, mikä ei olisi aivan ongelmatonta. Haitallisen disinformaation määritteleminen aukottomasti on äärimmäisen hankalaa. Ilman tarkkaa määritelmää palveluntarjoajat eivät kykene tietämään mikä kyetään laskemaan haitalliseksi disinformaatioksi. Jos verkkosivujen sisältöä alettaisiin sensuroimaan kansalliseen turvallisuuteen vedoten, ei mikään estäisi ajautumistamme Kiinan viitoittamalle mielivaltaisen sensuurin tielle. Suomen kyberturvallisuusstrategiassa (2019) todetaankin: "Suomi haluaa säilyttää universaalin, vapaan ja vakaan internetin ja mahdollistaa sen turvallisen käytön. Suomi ei hyväksy pyrkimystä rajoittaa internetin vapautta ja avoimuutta ja sitä kautta yksilön perusoikeuksia ja vapauksia."

Myös ihmisten laajamittainen kouluttaminen haitallisesta disinformaatiosta vaatisi käsitteen tarkan määritelmän. Määritelmän tulisi sisältää myös informaatiosodankäynnin ulkopuolinen, haitalliseksi laskettava disinformaatio, joka kykenee muodostamaan kyberuhkia. Vaikka tällainen määritelmä onnistuttaisiinkin kehittämään, vaatisi koko maan väestön kouluttaminen todella paljon resursseja. Valmistautuminen disinformaation muodostamien kyberuhkien torjuntaan on nykytilanteessa haastavaa, koska Suomessa ei olla tiettävästi varauduttu koko väestön kouluttamiseen kuin poikkeuksellisissa hätätilanteissa. Toisen merkittävän haasteen koulutukselle muodostavat eri väestöryhmien merkittävästi toisistaan poikkeavat tiedot ja valmiudet tietoliikennepalveluiden ja tietokoneiden yleisen käytön suhteen. Suuri osa vanhuksista ei käytä tietokonetta

edes pankkiasioidensa hoitamiseen (Tanskanen, 2011). Voidaan olettaa, että monien ihmisten tulisi ensin ymmärtää kybermaailmaan pohjautuvan informaationvälityksen perusteet, jotta he kykenisivät ymmärtämään näitä informaatiokanavia pitkin leviävän disinformaation muodostamat uhat.

Myös kohdennetussa mainonnassa käytettävät algoritmit muodostavat ongelman disinformaation haittavaikutusten ennaltaehkäisemisen kannalta. Internet-mainontaa tarjoavien yritysten on käytännössä mahdotonta varmistaa, etteivät heidän algoritmiensa kohdentamat mainokset johda käyttäjiä valeuutissivustoille. Vaikka kaikki mainokset tarkastettaisiinkin ihmisten toimesta ennen jakeluun pääsyä, eivät mainostajat kykene seuraamaan muuttuuko jo kerran tarkastetun sivuston sisältö myöhemmin valheelliseksi.

Ihmisten kouluttamisessa kyberturvallisuuden tiimoilta tulisi korostaa yksilötason kyberuhkia. Nykyisellään kyberturvallisuuden tutkimus keskittyy vahvasti organisaatiotasolle (Schatz ym., 2017), eikä Suomen kyberturvallisuusstrategiassakaan (2019) huomioida yksilöitä kuin koulutuksen osalta – uhat kohdistuvat edelleen lähtökohtaisesti yhteiskunnan tasolle. Yksilötason uhkien konkretisoiminen varoittavien esimerkkien avulla herättäisi ihmiset aihealueen vakavuuteen oletettavasti nykyistä tehokkaammin. Kohonnut yksilötason valmius haitallisen disinformaation tunnistamiseen näkyisi oletettavasti myös suoraan organisaatiotason puolustusvalmiudessa.

Suomen yleinen puolustusvalmius disinformaation muodostamien kyberuhkien torjuntaan vaikuttaa heikolta, koska valtiolla ei tiettävästi ole valmiuksia kouluttaa koko väestöä kattavasti kyberturvallisuuden tiimoilta. Haitallinen disinformaatio pääsee leviämään vapaasti kaikkien sellaisten ihmisten keskuudessa, joilla ei ole kykyä arvioida sen paikkansapitävyyttä.

4.2 Lähitulevaisuuden teknologisen kehityksen vaikutukset disinformaatiolta puolustautumiseen

Teknologioiden kehittyminen on niin sanotusti kaksiteräinen miekka haitalliselta disinformaatiolta puolustautumisen suhteen. Esimerkiksi sosiaalisen median läpimurto mahdollisti kohdennetun disinformaation levittämisen niin tehokkaasti, että informaatiosodankäynnin painopiste siirtyi disinformaation levittämiseen (Lei, 2019). Toisaalta Edward Snowdenin paljastukset Yhdysvaltojen ja muiden Five Eyes -liittoon kuuluvien valtioiden harjoittamasta massavalvonnasta todistavat, että teknologian kehittyminen on avannut täysin uusia ulottuvuuksia myös tiedustelutoiminnalle.

Kehittyvä teknologia avaa jatkuvasti uusia uhkia, jotka eivät ole aina ilmeisiä. Tästä syystä viranomaiset ovat käytännössä aina takamatkalla rikollisiin ja vihamielisiin tahoihin nähden pyrkimyksissään parantaa kyberturvallisuuden tilaa (Benzel, 2021). Lähitulevaisuudessa disinformaatiota saatetaan kyetä levittämään esimerkiksi Internet of Things -laitteiden kautta, kun yhä useammat arkiset laitteet kytketään internetiin (Sánchez-Torres, Rodríguez-Rodríguez,

Rico-Bautista & Guerrero, 2018). Uudet sosiaalisen median palvelut ja jatkuvasti kehittyvät tekoälypohjaiset mainontateknologiat avaavat myös uusia mahdollisuuksia kohdennetun disinformaation levittämiseen.

Kyberuhkien vakavuus on kuitenkin havaittu globaalissa mittakaavassa, ja niiden torjumiseen käytetään paljon resursseja. Yhdysvaltojen puolustusministeriön alaiset osastot kehittävät jatkuvasti uusia tekoälypohjaisia menetelmiä, joiden avulla disinformaatiota pyritään tunnistamaan, torjumaan ja hallinnoimaan. (Benzel, 2021). Smith, Kao, Mackin, Shah, Simek ja Rubin (2021) ovat kehittäneet tekoälypohjaisen sovelluksen, joka tunnistaa disinformaatiota levittävät käyttäjätunnukset erilaisissa palveluissa 96 prosentin tarkkuudella. Suuri osa puolustusteknologisista sovelluksista on salassapidettäviä, jotta kyberrikolliset ja vihamieliset tahot eivät kykenisi varautumaan niiden kiertämiseen.

5 YHTEENVETO

Informaatiosodankäynnin ulkopuolista disinformaatiota ei ole tiettävästi tutkittu kyberturvallisuuden näkökulmasta aiemmin. Tämä integroiva kirjallisuuskatsaus vastaa kysymyksiin: ”Millä perusteilla myös informaatiosodankäynnin ulkopuolinen disinformaatio saattaa muodostaa piilevän kyberuhan?” ja ”Kuinka yksilöt ja yhteiskunnat kykenevät puolustautumaan disinformaation muodostamilta kyberuhilta?”

Tämä kirjallisuuskatsaus kattaa 23 kappaletta Julkaisufoorumin luotettaviksi luokittelemissa julkaisuissa julkaistuja, vertaisarvioituja tieteellisiä artikkeleita. Disinformaation ja kyberturvallisuuden käsitteet on määritelty aiempien vertaisarvioitujen määritelmien pohjalta synteesiä muodostaen. Johtopäätökset tukevat aiempia, disinformaatiota ja yhteiskunnan sisäisen luottamuksen tilaa käsitteleviä tutkimuksia. Jo useat tutkijat ovat havainneet informaatiosodankäynnin ulkopuolisen disinformaation vaikutukset yhteiskunnan sisäiseen luottamukseen (Edwards, 2021). Tämän tutkielman kontribuutio on hajanaisten tutkimustulosten kokoaminen yhteen kyberturvallisuuden näkökulmasta tarkasteltavaksi kokonaisuudeksi.

Kybermaailmassa leviävän disinformaation määrän mittaaminen ja sen vaikutusten arvioiminen asettavat tutkijoille haasteita, koska ilmiöitä kyetään tutkimaan lähinnä mittaamalla yksittäisiä vaikutuksia, kuten yleisen luottamuksen kehittymistä. Täten on haastavaa osoittaa esimerkiksi harhaanjohtavan ja valheellisen viestinnän tarkkaa vaikutusta yleisen luottamuksen heikentymiseen. (Kavanagh & Rich, 2018, s. 40). Tutkielman lähdeaineistona käytetyt tilastot yhteiskunnan sisäisen luottamuksen heikentymisestä kuvaavat Yhdysvaltojen sisäisen luottamuksen kehitystä. Aihetta on haastavaa lähestyä Suomen näkökulmasta. Esimerkiksi OECD:n 4.5.2021 julkaisemassa raportissa Drivers of Trust in Public Institutions in Finland todetaan, että 66 % suomalaisista luottaa maamme hallitukseen. Raportin mukaan OECD:n jäsenmaissa keskimääräinen vastaava luottamus on 45 %. Julkaisufoorumi on kuitenkin määritellyt OECD:n epäluotettavaksi julkaisijaksi, joten tutkielmassa keskitytään Yhdysvaltoja käsitteleviin tilastoihin.

Disinformaatio heikentää yhteiskunnan sisäistä luottamusta, ja muodostaa kyberuhan, koska se leviää suurelta osin kybermaailmassa (Clapper, Lettre & Rogers, 2017). Disinformaatiopohjaista viestintää hyödynnetään esimerkiksi maineenhallinnassa, poliittisen kannatuksen keräämisessä ja mainonnassa. Tällaiset järjestelmällisen valehtelun muodot, joilla pyritään saavuttamaan henkilökohtaista etua, heikentävät ihmisten luottamusta perinteisiin informaatiolähteisiin, heikentäen yhteiskunnan sisäistä luottamusta samalla mekanismilla kuin informaatiosodankäynnin informaatio-operaatiotkin. (Edwards, 2021; Kavanagh & Rich, 2018, s. 62). Valtaosa nykyaikaisesta viestinnästä tapahtuu kybermaailman välityksellä. Näiden seikkojen pohjalta on perusteltua suhtautua tiedotus- ja viestintätoiminnalle ominaiseen disinformaatiopohjaiseen viestintään vähintäänkin piilevänä kyberuhkana, joka uhkaa yhteiskuntien sisäistä luottamusta.

Tehokkain tapa haitalliselta disinformaatiolta puolustautumiseen olisi koko maan kattava koulutus, joka opettaisi tunnistamaan haitallisen disinformaation ja reagoimaan siihen. Tämä vaatisi merkittävästi resursseja, ja koulutuksessa tulisi ottaa huomioon ihmisten väliset suuret erot tietoteknisissä tiedoissa ja valmiuksissa. Ennen koulutusta tulisi määritellä haitallinen disinformaatio tarkasti. Myöskään internetin palveluntarjoajien sisällön rajoittaminen ei onnistu ilman tarkkaa määritelmää. Valmiudet haitalliselta disinformaatiolta puolustautumiseen ovat tiettävästi heikot.

Jatkotutkimuksissa voitaisiin selvittää, millaisten keinojen avulla tarkoituksellisen harhaanjohtavaa viestintää kyettäisiin rajoittamaan, näin ennaltaehkäisten sen mahdollisesti luottamusta rappeuttavia vaikutuksia. Lainsäädännöllisen säätelyn ongelmaksi saattaisi muodostua tosiasiallisesti haitallisen disinformaation määritteleminen, koska tarkoituksellisen harhaanjohtamisen haitat ja hyödyt ovat subjektiivisia ja tapauskohtaisia.

Disinformaatiotutkimus ei ole vielä löytänyt menetelmää, jonka avulla kyettäisiin mittaamaan liikkeellä olevan disinformaation määrää. Myös sen vaikutusten arvioiminen on monimutkaista. (Kavanagh & Rich, 2018). Tällaisten mittaustapojen kehittäminen olisi luonteva askel aihealueen jatkotutkimuksen mahdollistamisen kannalta.

Kyberuhkien vaikutuksia yksilötasolla ei ole tutkittu käytännössä ollenkaan, koska tieteenala ei ole vielä löytänyt vastauksia yhteiskuntiakaan uhkaavien kyberuhkien saumattomaan torjumiseen. Yksilöiden kohtaamia kyberuhkia tulisi tutkia tarkemmin, ja voitaisiinko näitä ennaltaehkäisemällä helpottaa myös yhteiskunnan tasoisten uhkien torjuntaa.

Disinformaatio on luonteeltaan arvoneutraalia, ja sen levittäminen on vain yksi viestinnän väline, kuten Cunningham (1992) havaitsi perehtyessään propagandistisen viestinnän historiaan ja tutkimukseen. Osa propagandan määritelmää on, että tarkoituksellisella harhaanjohtamisella pyritään saamaan ihmiset käyttäytymään halutulla tavalla (Cunningham, 1992). Bernaysin (1942) mukaan harhaanjohtavan viestinnän eettisyyttä tulisi arvioida sen taustalla olevien motiivien eettisyyden pohjalta.

Kyberturvallisuuden kohentaminen edellyttää ihmisiltä kollektiivista kykyä haitallisen disinformaation tunnistamiseen ja siihen reagoimiseen. Jotta ihmisiä kyettäisiin valistamaan aiheesta, tulisi haitallinen disinformaatio kyetä ensin määrittelemään. Määritelmän tulisi sisältää myös informaatiosodankäynnin ulkopuolinen disinformaatio. Sekä harhaanjohtavassa tiedotus- ja suhdetoiminnassa että informaatiosodankäynnissä käytetään samanlaisia viestintätekniikoita, mutta niiden avulla pyritään saavuttamaan erilaiset päämäärät. Eriävistä motiiveistaan huolimatta molemmat viestintätavat ovat vaikuttaneet yhteiskuntien sisäisen luottamuksen heikentymiseen. Luottamusta perinteisiin informaatiolähteisiin on vaikeaa rakentaa uudestaan, jos niiden harjoittamaan järjestelmälliseen valehteluun ei suhtauduta haitallisena disinformaationa. Tämän tutkielman esiin nostama, piilevästi yhteiskunnan sisäistä luottamusta nakertava kyberuhka on päässyt muodostumaan vahingossa pitkäkestoisen järjestelmällisen valehtelun sivutuotteena.

LÄHTEET

Ackerman, S. (2016). James Clapper Resigns as US director of national intelligence. [uutisartikkeli] *The Guardian.* Haettu 18.5.2021 osoitteesta https://www.theguardian.com/us-news/2016/nov/17/james-clapper-resigns-director-national-intelligence.

Araźna, M. (2015). Conflicts of the 21st century based on multidimensional warfare – "hybrid warfare", disinformation and manipulation. *Security and defence quarterly, 8*(3), 103-129. Haettu osoitteesta https://doi.org/10.5604/23008741.1189421.

BBC. (2019). Cryptoqueen: How this woman scammed the world, then vanished. Haettu osoitteesta https://www.bbc.com/news/stories-50435014.

Benzel, T. (2021). Security: Cybersecurity Research for the Future. *Association for Computing Machinery. Communications of the ACM, 64*(1), 26. Haettu osoitteesta https://doi.org/10.1145/3436241.

Bernays, E. (1942). The Marketing of National Policies: A Study of War Propaganda. *Journal of Marketing, 6*(3), 236-244. Haettu osoitteesta https://doi.org/10.2307/1245869.

Bradshaw, S. (2019). Disinformation optimised: Gaming search engine algorithms to amplify junk news. *Internet policy review, 8*(Issue 4). Haettu osoitteesta https://doi.org/10.14763/2019.4.1442.

Browning, J. (2.3.2020). *Spying on the Scammer [Part ¼]*. [video]. Haettu osoitteesta https://www.youtube.com/watch?v=le71yVPh4uk.

Clapper, J., Lettre, M. & Rogers, M. (2017). Foreign Cyber Threats to the United States. *Hampton Roads International Security Quarterly, 1.* Haettu osoitteesta https://www-proquest-com.ezproxy.jyu.fi/docview/1865125438?pq-origsite=primo.

Cunningham, S. (1992). Sorting out the ethics of propaganda. *Communication Studies, 43*(4), 233. Haettu osoitteesta https://doi.org/10.1080/10510979209368375.

Curtis, A. (17.03.2002). *The Century of the Self* [dokumenttielokuva]. Haettu osoitteesta https://www.youtube.com/watch?v=eJ3RzGoQC4s.

Edwards, L. (2021). Organised lying and professional legitimacy: Public relations' accountability in the disinformation debate. *European journal of communication (London), 36*(2), 168-182. Haettu osoitteesta https://doi.org/10.1177/0267323120966851.

Fallis, D. (2015). What is disinformation? *Library Trends, 63*(3), p. 401. Haettu osoitteesta https://doi.org/10.1353/lib.2015.0014.

Hughes, H. & Waismel-Manor, I. (2021). *The Macedonian Fake News Industry and the 2016 US Election*. Cambridge University Press. Haettu osoitteesta https://doi.org/10.1017/S1049096520000992.

Innes, M. (2020). Techniques of disinformation: Constructing and communicating "soft facts" after terrorism. *British Journal of Sociology, 71*(2), 284-299. Haettu osoitteesta https://doi.org/10.1111/1468-4446.12735.

Jolley, D. & Douglas, K. M. (2014). The effects of anti-vaccine conspiracy theories on vaccination intentions. *PloS one, 9*(2), e89177. Haettu osoitteesta https://doi.org/10.1371/journal.pone.0089177.

Kavanagh, J. & Rich, M. (2018). *Truth Decay – An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life.* RAND Corporation, Santa Monica, Calif. Haettu osoitteesta https://www.rand.org/content/dam/rand/pubs/research_reports/RR2300/RR2314/RAND_RR2314.pdf.

Lei, H. (2019). Modern information warfare: Analysis and policy recommendations. *Foresight : the Journal of Futures Studies, Strategic Thinking and Policy, 21*(4), 508-522. Haettu osoitteesta https://doi.org/10.1108/FS-06-2018-0064.

Mcduffie, E. L. & Piotrowski, V. P. (2014). The Future of Cybersecurity Education. *Computer, 47*(8), 67-69. Haettu osoitteesta https://doi.org/10.1109/MC.2014.224.

OECD (2021), *Drivers of Trust in Public Institutions in Finland*, OECD Publishing, Paris. Haettu osoitteesta https://doi.org/10.1787/52600c9e-en.

Ryu, J., L'Espoir Decosta, J. & Andéhn, M. (2016). From branded exports to traveler imports: Building destination image on the factory floor in South Korea. *Tourism management (1982), 52*, 298-309. Haettu osoitteesta https://doi.org/10.1016/j.tourman.2015.07.004.

Sales, N. (2013). Regulating cyber-security. *Northwestern University Law Review, 107*(4), -1568. Haettu osoitteesta https://www-proquest-com.ezproxy.jyu.fi/docview/1499304970?pq-origsite=primo.

Sánchez-Torres, B., Rodríguez-Rodríguez, J., Rico-Bautista, D. & Guerrero, C. (2018). Smart Campus: Trends in cybersecurity and future development. *Revista FI-UPTC, 27*(47), 93-101. Haettu osoitteesta https://doi.org/10.19053/01211129.v27.n47.2018.7807.

Schatz, D., Bashroush, R. & Wall, J. (2017). Towards a more representative definition of cyber security. *The Journal of Digital Forensics, Security and Law : JDFSL, 12*(2), 53-74. Haettu osoitteesta https://search-proquest-com.ezproxy.jyu.fi/scholarly-journals/towards-more-representative-definition-cyber/docview/2035634435/se-2?accountid=11774.

Smith, S., Kao, E., Mackin, E., Shah, D., Simek, O. & Rubin, D. (2021). Automatic detection of influential actors in disinformation networks. *Proceedings of*

the National Academy of Sciences of the United States of America, 118(4), 1. Haettu osoitteesta https://doi.org/10.1073/pnas.2011216118.

Suomen Turvallisuuskomitea. (2019). Suomen kyberturvallisuusstrategia. Haettu osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf.

Taddeo, M. (2012). Information Warfare: A Philosophical Perspective. *Philosophy & Technology, 25*(1), p. 105-120. Haettu osoitteesta https://doi.org/10.1007/s13347-011-0040-9.

Taddeo, M. (2016). Just Information Warfare. *Topoi*, 35(1), p. 213-224. Haettu osoitteesta https://doi.org/10.1007/s11245-014-9245-8.

Tanskanen, M. (2011). *Ikääntyminen ja tietotekniikan oppiminen: "Kaikki uutta!"* (pro gradu -tutkielma, Jyväskylän yliopisto). Haettu osoitteesta https://jyx.jyu.fi/bitstream/handle/123456789/37168/1/URN%3ANBN%3Afi%3Ajyu-201201051012.pdf.

Taylor, P. (2013). *Munitions of the mind - A history of propaganda*. Manchester University Press. Haettu osoitteesta https://cryptome.org/2013/01/aaron-swartz/Mind-Munitions.pdf.

Verčič, D., van Ruler, B., Bütschi, G. & Flodin, B. (2001). On the definition of public relations: A European view. *Public relations review, 27*(4), 373-387. Haettu osoitteesta https://doi.org/10.1016/S0363-8111(01)00095-9.