Informaatioteknologian tiedekunnan julkaisuja
No. 98/2023

Isokangas, Jyrki (toim.)

Tiedustelun maailma: Muuttuva tiedustelu
Tiedusteluanalyysi I -kurssin raportteja

JYVÄSKYLÄN YLIOPISTO

Informaatioteknologian tiedekunnan julkaisuja
No. 98/2023

Toimitus: Jyrki Isokangas
Kannen kuva: iLexx, www.elements.envato.com

ISBN 978-951-39-9603-1 (verkkoj.)
ISSN 2323-5004

Jyväskylä 2023

Tiedustelun maailma: Muuttuva tiedustelu
Tiedusteluanalyysi I -kurssin raportteja

Jyrki Isokangas

2023

Sisällys

Esipuhe

Tiedusteluopetus on keskeinen osa Jyväskylän yliopiston Turvallisuus- ja strateginen analyysi -maisteriohjelmaa. Ensimmäisen vuoden opintoihin kuuluvassa strategisen tiedustelun moduulissa opiskelijat saavat ensikosketuksen tiedusteluun ja tiedusteluanalyysiin. Tiedusteluanalyysi I –kurssilla opiskelijat laativat ryhmätyönä raportin aiheeseen liittyvästä ilmiöstä. Raportit eivät perustu vielä tiedusteluanalyysiin, vaan niiden tavoitteena on syventää opiskelijoiden osaamista tiedustelusta. Syksyn 2022 kurssin ryhmätöistä on laadittu kaksi julkaisua. Toisen julkaisun teemana on Kiina. Tämä julkaisu käsittelee tiedustelun muutosta.

Tiedustelun muutosta tarkastellaan erilaisista näkökulmista. Ensimmäinen raportti käsittelee valtiollisen tiedustelumonopolin murtumista. Tiedustelu on ollut perinteisesti valtioiden omien tiedusteluorganisaatioiden tehtävä. Yhteiskunnan digitalisaatio on kuitenkin muuttanut asetelmaa, ja tiedustelusta on tullut myös liiketoimintaa. Lisäksi sosiaalinen media on mahdollistanut erilaisten tiedusteluanalyysiä tekevien yhteisöjen muodostumisen. Raportin mukaan kehitys asettaa perinteiset tiedustelupalvelut uusien haasteiden eteen.

Toinen raportti tarkastelee disruptiivisten teknologioiden vaikutusta tiedusteluun. Disruptiivisilla teknologioilla tarkoitetaan systeemitason toimintaa muokkaavia sovelluksia. Raportissa käsitellyt teknologiat - koneoppiminen, lohkoketjut, kvanttiteknologia ja esineiden internet - luovat tiedustelulle uusia mahdollisuuksia, mutta myös täysin uudenlaisia uhkia. Uudet teknologiat lisäävät tiedustelun suorituskykyä, mutta samalla niiden aiheuttamat riskit tulisi hallita.

Kolmannen raportin muutos liittyy tiedustelupalveluiden laajenevaan toimintaympäristöön. Se käsittelee Venäjän tiedustelupalveluiden toimintaa kyberympäristössä, avaten maan tiedustelupalveluiden toteuttamia kyberoperaatioita. Raportti muistuttaa, että Venäjän tiedustelupalvelut ja niihin liittyvät ryhmät eivät pelkästään kerää tietoa, vaan niillä on myös vaikuttamistehtäviä.

Neljäs raportti tarkastelee tiedustelun muuttuvia tehtäviä. Venäjän laajamittainen hyökkäys Ukrainaan helmikuussa 2022 toi tiedustelun julkisuuteen aikaisempaa näkyvämmin. Tiedustelun tehtävänä sodassa ei ole ollut pelkästään perinteinen päätöksenteon tukeminen, vaan tiedustelutietoa on käytetty myös informaatiovaikuttamiseen ja sen torjumiseen. Tiedustelun tuottamaa tietoa on käytetty myös ennaltaehkäisevästi Venäjän suunnittelemia operaatioita vastaan.

Julkaisun viimeisen raportin muutos koskee uhkakuvia. Suomeen kohdistuvien uhkien muutosta on tarkasteltu Suojelupoliisin vuosikirjojen kautta. Raportin mukaan uhkakuvat ovat muuttuneet vuosina 2015–2021 aikaisempaa monimuotoisemmiksi vaikeasti ennakoitavan toimintaympäristön takia. Taustalla vaikuttavat niin globaali kuin Suomen sisäinenkin kehitys.

Kaikki raportit on julkaistu opiskelijoiden luvalla. Julkaisun tarkoituksena ei ole syyllistää raporteissa käsiteltyjä maita tai organisaatiota, vaan niiden kautta opiskelijat ovat pystyneet syventämään omaa osaamistaan tiedustelusta.

Toivon mielenkiintoisia lukuhetkiä julkaisun parissa!

Jyväskylässä 19.4.2023
Yliopistonopettaja, FM, eversti evp. Jyrki Isokangas

Lyhenteet

3D	3-ulotteinen.
5G	Viidennen sukupolven mobiili datayhteys (engl. fifth generation).
6G	Kuudennen sukupolven mobiili datayhteys (engl. sixth generation).
APT	engl. Advanced Persistent Threat. Kehittyneitä ja edistyneitä kyberhyökkäyksiä tekevät ryhmät tai niiden operaatioiksi määritellyt hyökkäykset.
BBC	engl. British Broadcasting Corporation, Iso-Britannian julkinen yleisradio- ja tuotantoyhtiö.
BE3	engl. BlackEnergy 3. Haittaohjelma, jota levitetään sähköpostin Word- tai PowerPoint-asiakirjan liitetiedostona. Houkuttelee uhreja avaamaan tiedoston.
CERT	engl. Computer Emergency Response Team. Usein valtion tai ison organisaation tietoturvaloukkauksia käsittelevä organisaatio.
CITINT	engl. Citizen Intelligence, kansalaistiedustelu.
DCCC	engl. Democratic Congressional Campaign Committee. Yhdysvaltojen demokraattisen puolueen kongressikampanjakomitea.
DIIA	ukr. Deržava i Ja, valtio ja minä. Ukrainan valtionhallinnon tarjoama digitaalisten palvelujen mobiilisovellus ja verkkosivusto.
DNC	engl. Democratic National Committee. Yhdysvaltojen demokraattisen puolueen johtava elin.
EU	suom. Euroopan unioni.
FAPSI	ven. Federal'naya Agenstvo Pravitel'stvennoy Svayazi i Informatsii. Venäjän valtion viestintä- ja informaatiovirasto.
FSB	ven. Federal'naya Sluzhba Bezopasnosti Rossiyskoy Federatsii. Venäjän federaation turvallisuuspalvelu.
FSO	ven. Federal´naya Sluzhba Okhran. Venäjän federaation suojauspalvelu.
FVEY	engl. Five Eyes. Yhdysvaltojen, Iso-Britannian, Kanadan, Australian ja Uuden-Seelannin muodostama tiedusteluoperaatioiden liittouma.
GDPR	engl. General Data Protection Regulation, Euroopan unionin yleinen tietosuoja-asetus.
GEC	engl. Global Engagement Center. Yhdysvaltalainen virasto, jonka tehtävänä mm. johtaa ja ohjata propagandan ja disinformaation torjuntaa.
GEOINT	engl. Geospatial Intelligence, Geotiedustelu.
GNSS	engl. Global Navigation Satellite System. Satelliittipaikannusjärjestelmien yleisnimitys.
GPS	engl. Global Positioning System. Yhdysvaltalainen satelliittipaikannusjärjestelmä.
GRU	ven. Glavnoje Upravlenije General'nogo Shtaba Vooruzhonnykh sil Rossiyskoy Federatsii. Venäjän federaation asevoimien sotilastiedustelupalvelu.
GUR	ukr. Holovne Upravlinnia Rozvidky Ministerstva Oborony Ukrainy. Ukrainan sotilastiedustelupalvelu.
HUMINT	engl. Human Intelligence. Henkilötiedustelu.
IBM	engl. International Business Corporation. Kansainvälinen teknologiayritys.

IISS	engl. International Institute for Strategic Studies. Kansainvälinen tutkimusinstituutti.
IMINT	engl. Imagery Intelligence. Kuvaustiedustelu.
IoT	engl. Internet of Things. Esineiden internet. Järjestelmä, jossa toisiinsa yhteydessä olevat laitteet keräävät dataa ja kommunikoivat keskenään palveluiden tarjoamiseksi.
IP	engl. Internet Protocol. Internetin protokolla, joka huolehtii IP pakettien toimittamisesta tietokoneiden välillä.
IPv6	IP-protokollan versio, jonka avulla annetaan yksilölliset osoitteet internetissä toimiville laitteille.
LIDAR	engl. Light Detection and Ranging. Laserkeilaus.
MASINT	engl. Measurement and Signature Intelligence. Mittaus- ja tunnusmerkkitiedustelu.
MI6	engl. Military Intelligence, Section 6. Yhdistyneen kuningaskunnan ulkomaantiedustelupalvelu.
NAT	engl. Network Address Translation. Osoitteenmuunnos. Internet-tekniikka, jossa julkisesti liikennöityjä IP-osoitteita piilotetaan tai säästetään.
NATO	engl. North Atlantic Treaty Organization. Vuonna 1949 perustettu Pohjois-Atlantin puolustusliitto.
NSA	engl. National Security Agency. Vuonna 1952 perustettu Yhdysvaltojen signaalitiedusteluorganisaatio.
OECD	engl. Organization for Economic Co-operation and Development. Taloudellisen yhteistyön ja kehityksen järjestö.
OSINT	engl. Open Source Intelligence. Avointen lähteiden tiedustelu.
RCS	engl. Remote Control System. Tietokoneiden ja matkapuhelimien salakuuntelujärjestelmä.
RDP	engl. Remote Desktop Protocol. Microsoftin kehittämä protokolla. Graafinen käyttöliittymä, jonka avulla voidaan muodostaa yhteys toiseen tietokoneeseen verkkoyhteyden avulla.
SAR	engl. Synthetic Aperture Radar. Synteettisen apertuurin tutka. Tutkasäteilyyn perustuva jokasään kuvantamisen menetelmä.
SBU	ukr. Služba Bezpeky Ukrainy. Ukrainan turvallisuus- ja tiedustelupalvelu.
SCADA	engl. Supervisory Control And Data Acquisition. Ohjausjärjestelmäarkkitehtuuri koneiden ja prosessien korkean tason valvontaa varten. Käytetään esimerkiksi teollisuusprosessien ohjauksessa.
SIGINT	engl. Signals Intelligence. Signaalitiedustelu.
SSH	engl. Secure Shell. Salattuun tietoliikenteeseen käytetty protokolla, yleisesti käytössä etäkäyttöyhteyksissä.
SUPO	suom. Suojelupoliisi. Suomen sisäisen turvallisuuden palvelu, siviilitiedustelupalvelu.
SVR	ven. Sluzhba Vneshney Razvedki Rossiyskoy Federatsii. Venäjän federaation ulkomaantiedustelupalvelu.
UPS	engl. Uninterruptible Power Supply. Laite, jonka tehtävänä on taata tasainen virransyöttö lyhyissä katkoksissa ja syöttöjännitteen epätasaisuuksissa.
VPN	engl. Virtual Private Network. Laajentaa yksityisen verkon julkisen verkon yli. Käyttäjä voi lähettää ja vastaanottaa tietoja ikään kuin tietokone olisi suoraan yhteydessä yksityiseen verkkoon.

VALTIOLLISEN TIEDUSTELUMONOPOLIN MURTUMINEN

Antti Laulajainen, Anna Taivalmaa, Timo Vilén, Matias Virtanen

1 Johdanto

Tässä raportissa käsitellään valtiollisen tiedustelumonopolin murtumista ja siihen vaikuttaneita tekijöitä. Raportissa käydään läpi valtiollisen tiedustelumonopolin perustaa sekä syitä, miksi tiedustelutoiminta on historiallisesti ollut pääasiassa valtioiden harjoittamaa toimintaa, ja mitkä tekijät ovat vaikuttaneet tiedustelumonopolin murtumiseen. Raportissa tarkastellaan myös sitä, millaisia uusia toimijoita tiedustelun kentälle on tullut, ja millaisia motiiveja näillä toimijoilla on tiedustelutoiminnan harjoittamiselle. Lisäksi raportissa luodaan katsaus siihen, miten ei-valtiollisten toimijoiden tiedustelutoiminta näkyy Ukrainan sodassa.

Vaikka tiedustelutoimintaa on historiassa harjoitettu eri tavoin, ei tiedustelulle ole syntynyt yhtä yleisesti hyväksyttyä määritelmää. Erilaiset tiedustelutahot määrittelevät tiedustelun kukin omista lähtökohdistaan (Kari, 2020). Tiedustelu voidaan käsittää esimerkiksi prosessina, toimintana tai tuotteena (McDowell, 2009). On huomioitava, että erilaiset tiedustelun määritelmät eivät yleensä ota kantaa tiedustelua harjoittavaan tahoon: tiedustelua voivat harjoittaa esimerkiksi valtiot, yksittäiset ihmiset, yritykset sekä laillisesti ja laittomasti toimivat järjestöt ja ryhmät. Tässä raportissa tiedustelu ymmärretään sen laajassa merkityksessä, eli tiedustelu nähdään ennen kaikkea prosessina ja toimintana.

Raportin lähdemateriaalina on hyödynnetty akateemista tutkimuskirjallisuutta, harmaata kirjallisuutta sekä muita täydentäviä lähteitä, kuten uutisia. Raportissa pyritään löytämään vastaus seuraaviin kysymyksiin:

1. Mitkä tekijät ovat johtaneet valtiollisen tiedustelumonopolin murtumiseen?
2. Millaisia ei-valtiollisia toimijoita tiedustelun kentältä löytyy?
3. Miten valtiollisen tiedustelumonopolin murtuminen näkyy Ukrainan sodassa?

Raportin alussa kuvataan lyhyesti valtiollisen tiedustelumonopolin perusta ja eri tiedustelulajit. Tämän jälkeen käsitellään tiedustelumonopolin murtumiseen vaikuttaneita tekijöitä. Lisäksi tarkastellaan valtiollisten toimijoiden rinnalle tulleita tiedustelutoimijoita. Lopuksi käsitellään ei-valtiollista tiedustelutoimintaa Ukrainan sodan kontekstissa.

2 Valtiollinen tiedustelumonopoli ja sen murtuminen

Tiedustelua on totuttu pitämään valtioiden yksinoikeutena, monopolina. Tämä monopoli on kuitenkin murtumassa tai murtunut digitalisaation sekä erilaisten kaupallisten palveluiden, sensoreiden ja teknologioiden yleistymisen myötä. Tämä puolestaan on luonut uusia yhteisöjä, jotka tuottavat tiedustelutietoa valtioiden ohella tai kaupallisessa yhteistyössä valtioiden kanssa. Konkreettisesti tämä kehitys näkyy Ukrainan

sodassa ja sen tapahtumien seurannassa ja raportoinnissa. Seuraavat luvut käsittelevät mainittuja seikkoja tarkemmin.

2.1 Valtiollisen tiedustelumonopolin perusta

Tiedustelutoimintaa on harjoitettu eri muodoissaan tuhansien vuosien ajan, joskin nykyään tiedusteluksi käsitetty toiminta on muotoutunut 1800- ja 1900-lukujen aikana (McDowell, 2009). Tiedustelulla on ollut merkittävä rooli valtioiden välisten suhteiden hoitamisessa, ja tiedustelun merkityksen voidaan nähdä kasvaneen erityisesti viime vuosikymmenten aikana (Matovski, 2020). Kansainvälisten suhteiden ylläpidossa piilee kenties keskeisin syy valtiollisten tiedustelumonopolien synnylle, sillä valtiot ovat tarvinneet tietoa niin kumppaneistaan kuin vastustajistaankin. Valtiollisten tiedustelutoimijoiden tavoitteena on ollut tuottaa tätä tietoa asiakkailleen – eli valtiojohdolle – päätöksenteon tueksi (Gentry, 2016).

Valtiolliset tiedustelutoimijat ovat hyödyntäneet toiminnassaan kaikkia viittä tiedustelulajia eli henkilötiedustelua (HUMINT), avointen lähteiden tiedustelua (OSINT), signaalitiedustelua (SIGINT), mittaus- ja tunnusmerkkitiedustelua (MASINT) sekä geotiedustelua (GEOINT). Mahdollisuus eri tiedustelulajien hyödyntämiseen tiedustelutoiminnassa on osaltaan edesauttanut valtiollisia tiedustelutoimijoita niin kutsutun monopoliaseman saavuttamisessa.

Althoff (2016) kuvaa **henkilötiedustelua** tiedustelulajina, jossa tiedustelutiedon lähteenä on ihminen. Althoffin mukaan henkilötiedustelulle on ominaista keräystavan ja kerättävän aineiston salainen luonne sekä ihminen tiedon kerääjänä. Althoff myös korostaa henkilötiedustelun merkitystä muiden tiedustelulajien tuottaman tiedon perusteella havaittujen uhkien arvioimisessa.

Jardines'n (2016) mukaan **avointen lähteiden tiedustelulla** tarkoitetaan tiedustelutoimintaa, jossa tietoa kerätään nimensä mukaisesti avoimista lähteistä: tiedon tulee olla vapaasti saatavilla kenelle tahansa laillisia keinoja käyttäen, esimerkiksi pyytämällä, havainnoimalla tai ostamalla, ja tätä tietoa on mahdollista hankkia, tarkistaa ja analysoida tiedustelutehtävän suorittamiseksi. Jardines myös huomauttaa, että avointen lähteiden tiedustelu tukee muita tiedustelulajeja, mutta ei kuitenkaan voi täysin korvata niitä.

Nolte (2016) kuvaa **signaalitiedustelulla** tarkoitettavan elektronisesti välitetyn datan ja informaation keräämistä ja prosessointia tiedustelutarkoituksiin. Hänen mukaansa signaalitiedustelun avulla kerätään tietoa ihmisten välisestä elektronisesta viestinnästä sekä muista elektronisista signaaleista, kuten tutkasignaaleista.

Mittaus- ja tunnusmerkkitiedustelulla tarkoitetaan tiedustelun kohteesta kerätyn datan ja sen muutosten havainnointia ja analysointia, kuten muutoksia kohteen säteilytasossa ja maan värähtelyssä esimerkiksi räjähdysten vuoksi (West, 2015).

Geotiedustelu puolestaan määritellään Murdockin ja Clarkin (2016) mukaan usein kuten se on määritelty Yhdysvaltain lainsäädännössä, jossa geotiedustelulla tarkoitetaan kuvien, kuvaustiedustelun ja paikkatietojen avulla kerättyä tietoa (10 U.S.C. §467).

On huomattava, että teknologian kehityksellä on ollut vaikutusta siihen, miten ja missä määrin eri tiedustelulajeja on hyödynnetty tiedustelutoiminnassa: esimerkiksi nykymuotoinen geotiedustelu on mahdollistunut pitkälti kuvausteknologian kehityksen myötä. Teknologinen kehitys on toisaalta vaikuttanut myös siihen, miten eri toimijat ovat voineet eri tiedustelulajeja hyödyntää. Toisaalta esimerkiksi henkilötiedustelu on

ollut myös ei-valtiollisten toimijoiden suosiossa, mihin on saattanut vaikuttaa henkilötiedustelun hyvä kustannus-hyötysuhde. Henkilötiedustelu ei myöskään välttämättä vaadi mittavia taloudellisia panostuksia esimerkiksi teknologiaan (Althoff, 2016).

Ewingin (2022) mukaan keskeisimpiä syitä valtioiden monopoliasemalle tiedustelutoiminnassa ovat esimerkiksi lainsäädäntövalta, informaatioympäristön hallinta ja kattavat tiedustelutietoarkistot. Valtioilla on näin ollen ollut muita toimijoita paremmat mahdollisuudet vaikuttaa siihen kenen toimesta, miten ja missä tiedustelutoimintaa harjoitetaan. Monopolin keskeisimpänä historiallisena perustana on ollut valtioiden määräysvalta, ei niinkään paremmat resurssit tai teknologiat.

2.2 Valtiollisen tiedustelumonopolin murtumiseen vaikuttavia tekijöitä

Digitalisaatio ja sen mahdollistajana toimiva teknologian kehitys on johtanut tilanteeseen, jossa on aiempaa enemmän laitteita tiedon tuottamiseen ja etsimiseen sekä käsittelemiseen, sekä helposti saatavilla entistä suuremmalle joukolle ihmisiä. Samalla tuotetun tiedon määrä on moninkertaistunut helpon tallentamisen ja jakamisen kautta. Teknologian kehitys on synnyttänyt tiedustelupalveluiden rinnalle kansalaisten tiedonkeräysyhteisöjä ja yritysten kaupallisia palveluita. Myös tiedon analysointiin keskittyviä yhteisöjä on muodostunut harrastuspiirien tiedonvaihdon helpottumisen kautta, minkä lisäksi on syntynyt kokonaan uusia yhteisöjä analysoimaan kerättyä tietoa. Tiedustelupalveluilla on vielä tietolähteitä ja teknologioita, jotka eivät ole julkisesti saatavilla, mutta ei enää monopoliasemaa kaikkeen tietoon.

Postmodernia yhteiskuntaa leimaavat tiedon pirstoutuminen, globalisaatio sekä yhteisen narratiivin hiipuminen ovat asettaneet myöhäismodernina aikana syntyneet tiedustelupalvelut uuden tilanteen eteen. Muutos uuteen todellisuuteen on vääjäämätöntä ja jo osittain tapahtunut. Postmoderni tiedustelu on syntymässä, eikä tiedustelu enää toimi yksinoikeudella yhden narratiivin mukaan. Digitalisaatio ja teknologian kehitys ovat muuttaneet tiedustelupalveluita ja toimintatapoja peruuttamattomasti.

2.2.1 Digitalisaatio ja teknologinen kehitys

Valtiollisen tiedustelumonopolin murtumiseen on erityisesti vaikuttanut yhteiskunnassa tapahtuva digitalisaatio. Yhteiskunnan perustoiminnot ovat suuressa määrin muuttuneet digitaalisiksi. Kommunikaatio viranomaisten ja kansalaisten välillä on mahdollista pelkästään digitaalisessa muodossa, ja arkipäiväinen ihmisten välinen kanssakäyminen on myös lisääntyvissä määrin muuttunut digitaaliseen muotoon. Pelkän puheen tai tekstin sijasta tai niiden lisänä voidaan lähettää kuvia, tiedostoja tai suoraa videokuvaa.

Digitalisaation on mahdollistanut teknologian kehitys kohti ubiikkia, kaikkialla läsnä olevaa tietojenkäsittelyä, jossa äly on hajautunut arkisiin laitteisiin (Peltonen, 2018). Digitaalinen, ubiikki yhteiskunta vaatii toimiakseen edullisia helppokäyttöisiä päätelaitteita, joilla palveluita voidaan käyttää, sekä luotettavia palveluja tuottavia laitteita, jotka säilövät ja välittävät tietoa.

Laitteiden kehityksen lisäksi tiedon olomuoto on muuttunut. Lähes kaikki tieto tuotetaan suoraan digitaliseen muotoon, ja vaikka se julkaistaisiin muussa muodossa, on tieto jossain vaiheessa elinkaarta ollut digitaalisessa muodossa. Todennäköisesti lopullinen versio tallennetaan digitaaliseen muotoon tietovarastoon. Digitaalisessa muodossa oleva tieto on entistä helpommin kaikkien saatavilla. Erityisesti tiedon saatavuuteen ovat vaikuttaneet hakukoneet, jotka indeksoivat valtavan määrän tietoa päivittäin.

Näiden avulla tieto on löydettävissä helposti, mukaan lukien julkaisujen vanhat poistetut versiot. Voidaankin todeta teknologisen kehityksen ja tiedon digitaalisen olomuodon toimivan digitalisaation moottorina ja näin osaltaan murtavan tiedustelumonopolia.

Teknologian kehitys ja erityisesti informaatioteknologian kehitys ovat suurimpia vaikuttimia tiedustelumonopolien murroksessa. Internetin saatavuuden yleistyminen, älykkäiden mobiililaitteiden kehitys ja siihen yhdistyvät langattomat yhteydet ovat keskeisiä tekijöitä monopolin murroksessa. Bargerin (2005) mukaan informaatioteknologia ja sen kehitys on muuttanut yhteiskuntia radikaalisti. Tiedon jakamisen helppous ja lähes reaaliaikaisuus on mahdollista teknologisen muutoksen vuoksi.

Samaan aikaan teknologinen kehitys on siirtynyt vahvasti valtioilta yksityisille yrityksille. Esimerkiksi Yhdysvalloissa teknologiset läpimurrot ovat olleet jo 1980-luvulta lähtien peräisin yksityisiltä yrityksiltä, joiden tuotteita käytetään laajalti kaikessa toiminnassa, myös tiedustelupalveluissa (Barger, 2005). Yksityiset yritykset ovat erityisen näkyvästi edistäneet mobiililaitteiden kehitystä ja niiden käytön leviämistä globaalisti.

Mobiililaitteiden kehitys on tärkeimpiä tiedustelumonopolin murtumista selittäviä ilmiöitä. Mobiililaitteet kykenevät toimimaan helppokäyttöisinä sensoreina ja tiedonjakelijoina. Guo ym. (2015) mukaan mobiililaitteet muodostavat tehokkaan sensori- ja laskentaverkon, joka pystyy keräämään tietoa sekä tietoverkkoon kytkettynä että kytkemättömänä. Laitteilla kerättyä tietoa voidaan hyödyntää esimerkiksi geotiedustelussa. Mobiililaitteen ollessa kytkettynä tietoverkkoon, on sensoritiedon jakaminen nopeaa ja lähes reaaliaikaista hyödyntämällä sosiaalisen median palveluita.

Mobiililaitteet sisältävät kehittynyttä teknologiaa ja valmiita sensoreita, jotka aiemmin eivät olleet kuluttajien saatavilla. Sensoreita, kuten esimerkiksi laserkeilaukseen käytettäviä LIDAR-sensoreita, on jo kuluttajatason mobiililaitteissa, joiden toimivuutta on testattu historiallisten kohteiden kuvantamisessa (Teppati Losè ym., 2022). Mobiililaitteiden lisäksi on mahdollista hankkia kohtuuhintainen drone LIDAR-sensoreilla ja tulosten tulkitsemisessa käytettävällä sovelluksella pakettina verkkokaupasta (Alibaba.com, 2022).

Tiedon jakamisen helppous on muodostanut yhteisöjä, jotka tekevät analyyseja saatavilla olevista tiedoista tai kannustavat harrastajia jakamaan keräämänsä tietoa. Bargerin (2005) mukaan teknologian kehityksen mukana syntyneiden informaatioyhteisöjen on jopa esitetty olevan kyvykkäämpiä analysoimaan tiettyjä uhkia, kuten kansalaislevottomuuksien syntyä, ympäristöuhkia ja terveyskriisejä, kuin perinteinen tiedusteluyhteisö.

2.2.2 Postmoderni tiedustelu

Tiedustelupalvelujen muuttumista yhteiskunnan muutoksien mukana voidaan tarkastella postmodernin sosiaalisen teorian kannalta. Edellisessä luvussa käsitelty teknologian muutos katsotaan olevan moottori postmodernin yhteiskunnan kehityksessä (Rathmell, 2002). Teknologinen muutos vaikuttaa yhteiskunnan lisäksi myös tiedustelupalveluihin, jolloin on mielekästä tarkastella tiedustelun muutosta kohti postmodernia tiedustelua pois jälkiteollisista modernismin rakenteista.

Käsitteenä Rathmellin (2002) mukaan postmodernismi viittaa uusien näkökulmien syntymiseen suhteessa tietoon ja prosesseihin joissa luodaan tietoa. Rathmell jatkaa, että kyse on huomattavista muutoksista taloudellisesti ja teknologisesti, jotka vaikuttavat myös sosiaalisiin rakenteisiin ja yksilöihin. Postmodernismille voidaan Rathmellin mukaan määritellä viisi ydinteemaa: suurien narratiivien loppu, absoluuttisten

totuuksien etsimisen lopettaminen, puuttuvat keskustat ja epävarmat identiteetit, liikkuvat rajanvedot ja osaamistalous. Teemoja on avattu tarkemmin liitteessä 1.

Rathmellin (2002) mukaan yksi dramaattisimmista modernismin ajan tiedustelupalveluihin kohdistuneista muutoksista ollut kylmän sodan loppuminen. Tiedustelupalvelut olivat kylmän sodan muotoilemina salamyhkäisiä, irrallaan yhteiskunnasta, korostivat salaista ja usein teknistä tiedonkeräystä ja tyytyivät lineaarisiin ennustaviin päättelyihin. Kylmän sodan loppuminen yhdessä teknologian muutoksen kanssa, on ajanut tiedustelupalveluita kohti postmodernismia ja valtiollisen monopolin murtumista.

Rathmellin (2002) mukaan tarkasteltaessa postmodernin teorian käytön sopivuutta arvioimaan nykyisiä länsimaisia tiedustelupalveluja ja niiden tilaa, on tätä varten muodostettava omat postmodernin tiedustelun ydinteemat. Teemojen rakentaminen on mahdollista yhdistämällä tiedustelupalveluissa tapahtuviin muutoksiin postmodernin teorian ydinteemat. Rathmell esittääkin postmodernin tiedustelun ydinteemoiksi seuraavia seikkoja: kohteiden, roolien ja tehtävien pirstoutuminen, “arvoituksia ei palapelejä”, identiteetti, häilyvät raja-aidat sekä tiedustelutehtaan loppu. Teemat on esitelty liitteessä 2.

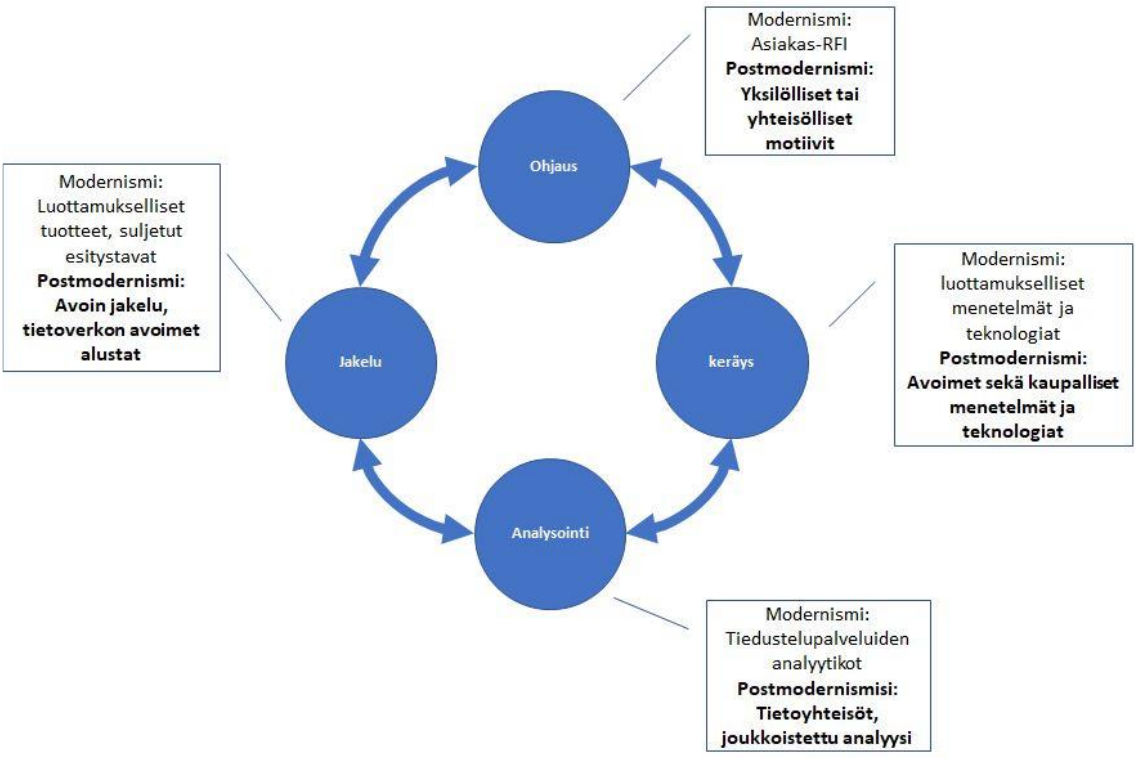
Teemoista erityisesti häilyvät raja-aidat soveltuvat hyvin kuvaamaan tiedustelumonopolin murrosta. Teemassa on määritelty, kuinka teknologia ja osaaminen, joka ennen oli luottamuksellista ja pelkästään tiedustelupalvelujen käytössä, on siirtynyt myös yksityisen sektorin käyttöön. Samalla valmiiden kaupasta ostettavien tuotteiden käyttö tiedon keräämisessä ja analysoinnissa on lisääntynyt ja siten ei-valtiollisten osaamisyhteisöjen kyvykkyys on lähentynyt kansallisia tiedustelupalveluiden kyvykkyyksiä.

2.2.3 Tiedustelumonopolin murros tiedustelusyklin näkökulmasta

Tarkasteltaessa tiedustelumonopolin murtumista tiedustelusyklin näkökulmasta, voidaan siihen liittää postmodernin tiedustelun ydinteemoja. Kokonaisuutena tiedustelun muutosta ja monopolin murtumista ajaa postmodernin tiedustelun ydinteema: tiedustelutehtaan loppu. Rathmellin (2002) mukaan tietotalouden nousu, teknologian ja sosiaalisen muutoksen voimalla, muuttaa tiedustelutoimintaa tai -taloutta samoin kuin muutakin yhteiskuntaa. Samalla muuttuvat tiedustelusyklin eri vaiheiden taustatekijät, itse syklin muuttuessa yhä joustavammaksi ja itseään iteroivaksi tietoyhteiskunnan tai -talouden mukaisesti.

Ohjausvaiheessa modernin tiedustelun asiakkaan tietopyyntö muovautuu motiivilähtöiseksi tiedon hankinnaksi, pirstaloituneen kohteiden ja mysteerien, “ei palapelejä” -teemojen mukaisesti. Myös identiteetin muutos -teema vaikuttaa tietopyyntöön. Tiedon keräys luottamuksellisilla menetelmillä ja teknologioilla vaihtuu raja-aitojen hämärtymisen -teeman mukaisesti avoimien menetelmien ja kaupallisten teknologioiden avulla tehtäväksi keräykseksi.

Tiedon analysointi tiedustelupalvelun analysoijien tekemänä muuttuu samasta syystä tietoyhteisöjen analyysiin ja joukkoistettuun analyysiin. Vastaavasti tiedustelutuotteen jakelu muuttuu luottamuksellisesta jakelusta ja suljetuista esityksistä avoimeen jakeluun ja tietoverkon avointen palvelujen hyödyntämiseen. Kuvio 1 esittää postmodernin tiedustelusyklin, mukaillen Rathmellin (2002) esittämiä postmodernin tiedustelun ydinteemoja.



KUVIO 1 Postmoderni tiedustelusykli Rathmellia mukaillen (Rathmell, 2002)

Syklin eri vaiheet ovat vahvasti takaisinkytkeytyviä ja syöttävät tietoa eri vaiheiden välillä entistä enemmän. Syklin vaiheissa on enemmän kytkentöjä myös tiedustelupalvelun ulkopuolisille toimijoille, jotka myös syöttävät tietoa tiedustelusykliin. Tiedustelusyklin tuloksena syntyvä tiedustelutuote on siten tuotos, jossa on aiempaa enemmän tiedustelupalvelun prosessien ulkopuolista dataa ja jopa osittain yhteisöllisesti tuotettua analyysia. Todennäköisesti tämä myös vaikuttaa tuotteen osittaiseen jakeluun avoimilla alustoilla.

2.3 Ei-valtiollisia tiedustelutoimijoita

Seuraavassa luodaan katsaus tiedustelun kentältä löytyviin ei-valtiollisiin toimijoihin. Katsaus ei pyri olemaan kattava, vaan lähinnä nostamaan esiin aihepiirin kannalta keskeisimpiä ei-valtiollisia toimijoita.

2.3.1 Kaupalliset tiedusteluyritykset

Erilaisia kaupallisia tiedusteluyrityksiä voidaan yrittää ryhmitellä tiedustelusyklin näkökulmasta. Osa yrityksistä – varsinaiset tiedusteluyritykset sekä osa teknologiayrityksistä – kattavat toiminnallaan koko tiedustelusyklin, ohjauksesta tiedustelutuotteiden jakamiseen, kun taas osa yrityksistä keskittyy pelkästään keräykseen, esimerkiksi kuvaustiedusteluun, tai erilaisten sensoreiden ja muiden laitteiden kehittämiseen ja myymiseen (Meier, 2021).

Ensin mainittuun ryhmään kuuluvia yrityksiä on ollut olemassa jo pitkään. Esimerkiksi sotilaalliseen ja uhkatiedusteluun keskittynyt Janes Information Services on toiminut yhtäjaksoisesti aina vuodesta 1898. Janes tarjoaa asiakkailleen valmiita katsauksia

ja datasettejä mm. eri valtioiden puolustushankinnoista ja sotilaallisista kyvykkyyksistä. Lisäksi tarjolla on räätälöidympiä ratkaisuja ja konsultointia (Janes, 2022).

Monet tiedustelualan yrityksistä harjoittavat myös henkilötiedustelua, osa avoimemmin (keskustelu ja havainnointi) ja osa myös peitellymmin (esim. peiteoperaatiot, soluttautumiset, tietomurrot, disinformaatiokampanjat). Esimerkin avointa strategista henkilötiedustelua harjoittavista yrityksistä tarjoaa Orbis Business Intelligence Ltd, jonka perustaja, entinen MI6:n tiedustelu-upseeri Christopher Steele tunnetaan paitsi kuuluisasta raportistaan, myös kattavista kontaktiverkostoistaan (Orbis, 2022; Meier 2021).

Israelilaislähtöinen Black Cube taas on tullut tunnetuksi peiteoperaatioistaan (Black Cube, 2022). Black Cube muistuttaa toimintatavoiltaan perinteisiä etsivätoimistoja kuten Pinkerton, mutta sitä on kuvattu myös ”liikemaailman Mossadiksi”, koska monet yrityksen perustajista ja työntekijöistä ovat Israelin siviili- ja sotilastiedustelupalveluiden veteraaneja (Hirshorn, 2018). Yritys nousi otsikoihin elokuvatuottaja Harvey Weinsteinin seksuaalirikosjutun yhteydessä, ja on joutunut kohujen keskelle myös kotimaassaan Israelin puolustusministeriön turvauduttua sen palveluihin (Azulai, 2019; Megiddo, 2019). Kuten yksityisiä tiedusteluyrityksiä tutkinut Barry Meier (2021) muistuttaa, valtiollisten ja kaupallisten tiedustelutoimijoiden yhteistyö ei sinällään ole harvinaista – pikemminkin päinvastoin, sillä valtiolliset toimijat voivat palkata yrityksiä tekemään asioita, joita ne itse eivät voi tai halua tehdä.

Tiedusteluyrityksiksi voitaneen laskea myös datan louhintaan, psykologiseen profilointiin ja strategiseen kommunikaatioon keskittyvät yritykset. Näistä tunnetuin lienee brittiläinen SCL Group. Sen tytäryhtiö, nyttemmin toimintansa lopettanut Cambridge Analytica, muistetaan paitsi läheisistä suhteistaan Yhdysvaltain ja Ison-Britannian poliittiseen eliittiin, myös osallistumisestaan Donald Trumpin sekä lukuisten muiden kiistanalaisten poliitikkojen vaalikampanjoihin (Jungherr, Rivero Rodríguez Gonzalo & Gayo-Avello, 2020).

Myös Microsoftin ja Googlen tapaiset isot teknologiayhtiöt on mainittava tässä yhteydessä, ei pelkästään valtioiden tiedustelumonopolin romahtamiseen johtaneen kehityksen vauhdittajina, vaan myös itsenäisinä tiedustelutoimijoina. Ukrainan sodan myötä on myös enenevässä määrin herätty teknologiajättien merkitykseen kansalliselle ja kansainväliselle turvallisuudelle. Tutkija Klon Kitchen onkin kuvannut tilannetta toteamalla, että “olemme kaikki nykyisin turvallisuusbisneksessä” (Reagan Foundation, 2022).

Teknologisen kehityksen etujoukoissa perinteisesti kulkeneet valtiolliset tiedustelupalvelut ovat myös joutuneet myöntämään, etteivät niiden resurssit enää riitä kilpailemaan isojen teknologiayhtiöiden kanssa. Tämä on osaltaan kannustanut läntisiä tiedustelupalveluita muodostamaan uusia kumppanuuksia teknologiayhtiöiden sekä laajemmin akateemisen yhteisön kanssa. Tämä on johtanut tilanteeseen, jota MI6:n nykyinen johtaja Sir Richard Moore (2021) on kuvannut paradoksaaliseksi: lähtökohtaisesti salaisten tiedustelupalveluiden täytyy Mooren mukaan ”muuttua avoimemmiksi voidakseen pysyä salaisina”.

Osa kaupallisista tiedustelutoimijoista keskittyy suomalaisen Iceyen tavoin erilaisten kuvaustiedustelutuotteiden myymiseen. Yhtiön kehittämillä, SAR-tutkia hyödyntävillä mikrosatelliiteilla voidaan tuottaa miltei reaaliaikaista tutkakuvaa vaikkapa tulvatuhojen tai maanjäristysten arvioimiseksi (Iceye, 2022b). Asiakkaina on mm. vakuutusyhtiöitä, mutta Iceye on myös tehnyt Ukrainan asevoimien kanssa sopimuksen, jonka nojalla Ukrainan sotilastiedustelu voi hyödyntää yrityksen tuottamaa satelliittikuvaa (Iceye, 2022a).

Myös erilaisia sensoreita, häirintä- ja salakuuntelulaitteita tai -ohjelmistoja myyviä yrityksiä löytyy runsaasti. Uusien, laillisilta tai laittomilta markkinoilta saatavien teknologioiden ansiosta kuka tahansa, jolla on riittävästi rahaa, tahtoa tai osaamista, voi nykyisin hankkia käyttöönsä signaalitiedustelun ja kuvaustiedustelun kyvykkyyksiä, joita aikaisemmin löytyi vain kansallisvaltioilta (Wein-baumm, Berner & McClintock, 2017).

Esimerkistä käy Hacking Team nimisen yrityksen tarjoama Remote Control Systems (RCS). Palvelu mahdollistaa tietokoneiden ja puhelimien salakuuntelun, ja sen saa käyttöönsä 200 000 dollarin vuosittaista lisenssiä vastaan. Toisaalta vaatimattomampaan tiedustelukäyttöön tarkoitettuja vakoiluohjelmia saa muutamilla kympeillä, ellei sitten halua kehittää sellaista itse. Tunnetun esimerkin tarjoaa venäläinen, aikanaan 26 dollaria maksanut SkyGrabber-ohjelma, jonka avulla irakilaiset hakkerit onnistuivat kaappaamaan Yhdysvaltain armeijan miehittämättömän Predator-lennokin välittämää videokuvaa (Weinbaumm, Berner & McClintock, 2017).

2.3.2 Rikollisjärjestöt ja terroristiorganisaatiot

Erilaiset rikollisryhmittymät (huumekartellit, kyberrikolliset jne.) samoin kuin terroristijärjestöt ovat valtiollisten tiedustelupalveluiden uhkatiedustelun perinteisiä kohteita – mutta kuten yllä jo viitattiin, ne ovat myös itsenäisiä tiedustelutoimijoita, jotka ovat voineet kehittää omia kyvykkyyksiään tiedustelun demokratisoitumisen ansiosta.

Keinot ja valmiudet ovat osin samoja kuin kaupallisten yritysten tiedusteluanalyytikoilla tai tutkivilla journalisteilla, joskin valmius hyödyntää harmaiden ja pimeiden markkinoiden tuotteita ja palveluita sekä kyberosaaminen saattavat nostaa rikollisjärjestöjen kyvykkyydet valtiollisten toimijoiden luokkaan etenkin kybertoimintaympäristöstä puhuttaessa. Meksikon huumekartellien tiedetään esimerkiksi hyödyntäneen yllä kuvattua Remote Control Systemsiä huumerikollisuudesta raportoivien paikallisten toimittajien seuraamiseen (Weinbaumm, Berner & McClintock, 2017; Guardian, 2020).

2.3.3 Kansalais- ja avustusjärjestöt

Erilaiset avustus- ja kansalaisjärjestöt on perinteisesti liitetty tiedusteluun valtiollisten tiedusteluelinten tietolähteinä. Ne ovat myös pitkään keränneet ja analysoineet tietoa omiin tarpeisiinsa. Esimerkiksi Punaisen Ristin on olennaista pystyä arvioimaan henkilöstöönsä ja operaatioihinsa kohdistuvia uhkia, olkoonkin, ettei tätä prosessia ole perinteisesti haluttu kutsua tiedusteluksi termin latautuneisuuden takia (MacLeod, 2009).

Kansainvälisten kriisien monimutkaistuminen sekä tiedustelun demokratisoituminen ovat myös kannustaneet avustusjärjestöjä panostamaan lisää tiedusteluun. Apua on haettu kaupallisilta yrityksiltä, samalla kun järjestöt ovat alkaneet kehittää omia kyvykkyyksiään tiedustelutiedon keräämiseksi ja analysoimiseksi. Tätä on pidetty tärkeänä myös järjestöjen toimintavapauden kannalta: ilman omaa, riittävän hyvää tiedustelutietoa ne ovat riippuvaisia paikallisten toimijoiden (hallitus, armeija, turvallisuuspalvelut, paikalliset rikollisjärjestöt jne.) tarjoamasta tiedosta, mihin sisältyy muitakin ilmeisiä riskejä kuin järjestöjen puolueettomuuden vaarantuminen (Whitford & Prunckun, 2017; Zwitter, 2016).

2.3.4 Tutkijat, tutkivat journalistit, kansalaisjournalistit ja kansalaistiedustelu

Akateemisen maailman suhde tiedusteluun on aina ollut läheinen. Tiedustelupalveluiden työntekijöitä on rekrytoitu suoraan eliittiyliopistojen penkeiltä, ja toisen maailmansodan aikana esimerkiksi yliopistojen venäjän kielen professorit antoivat tärkeän

panoksensa sotilastiedustelun hyväksi, myös Suomessa. Myös signaalitiedustelun puolella yliopistojen ja muotoaan hakevien tiedustelupalveluiden välinen yhteistyö on ollut tiivistä (Andrew, 2018; Porvali, 2022).

Internetin sekä sensoriteknologian kehityksen myötä akateemiset tutkijat ovat kuitenkin enenevissä määrin siirtyneet valtiollisten tiedustelupalveluiden perinteisesti hallitsemalle tontille jo normaalioloissa. Esimerkiksi joukko amerikkalaisia tutkijoita onnistui loppukesästä 2021 avoimia lähteitä sekä kaupallisia satelliittikuvia hyödyntämällä löytämään uusia kiinalaisia ohjussiiloja ja näin osoittamaan, että Kiina oli laajentanut merkittävästi ohjusarsenaaliaan (Ewing, 2022).

Se, mitä yllä on sanottu akateemisista tutkijoista ja tiedustelun demokratisoitumisesta pätee luonnollisesti myös tutkivaan journalismiin sekä kansalaisjournalismiksi kutsuttuun ilmiöön. Sen tunnetuimpana edustajana voitaneen pitää vuonna 2014 perustettua Bellingcat-verkostoa, joka on erikoistunut vakavien rikosten, erityisesti sotarikosten, sekä erilaisten rikollisverkostojen tutkimiseen. Bellingcatin verkkosivujen tietopankkiin on koottu kymmeniä tuhansia sosiaalisen median julkaisuja, jotka verkoston vapaaehtoiset ovat luokitelleet ja geopaikantaneet satelliittikuvien ja Google Street View:n avulla. Aloitteleville tutkijoille tarjotaan myös ohjeita sekä erilaisiin OSINT-työkaluihin ja -menetelmiin keskittyviä työpajoja (Bellingcat, 2023).

Bellingcatin tekemät selvitykset Sergei Skripalin ja Aleksei Navalnyin salamurhayrityksistä, malesialaisen MH-17-koneen alas ampumisesta sekä lukuisista muista sotarikoksista ovat osoittaneet joukkoistetun tiedustelun voiman sekä nostaneet julkisuuteen asioita, joista valtiolliset toimijat ovat voineet keskustella vain rajoitetusti. Ne ovat myös asettaneet perinteiset tiedustelupalvelut valinnan eteen: Pitäisikö tutkijoiden toimintaa yrittää suitsia? Vai olisiko parempi vaieta tai hakeutua yhteistyöhön? Ja jos yhteistyöhön, niin millä tavalla ja millä tasolla yhteistyötä voitaisiin tehdä? Tarjoamalla rahoitusta tai uusia lähteitä? Perustamalla yhteistyöfoorumeita? Vai pelkästään signaloimalla – hienovaraisemmin tai suoraan – että tutkijat ovat oikealla asialla? (Ewing, 2022)

Aiemmin mainitussa, Kiinan ohjussiiloja koskevassa tapauksessa USSTRATCOM:in (engl. United States Strategic Command) amiraali Charles Richard kannusti tutkijoita jatkamaan toteamalla lehdistökonferenssissa: “Jos teistä on mukavaa katsella kaupallisia satelliittikuvia tai kiinalaista kamaa, niin saanko ehdottaa, että jatkatte katselemista?” (Ewing, 2022)

Kansalaisjournalismin lisäksi puhutaan CITINT:istä (engl. citizen intelligence), siis kansalaistiedustelusta tai joukkoistetusta tiedustelusta. Jälkimmäinen on läheistä sukua kansalaisjournalismille, mutta keskittyy tiedustelutiedon joukkoistettuun keräämiseen. Esimerkiksi Ukrainassa tavalliset ihmiset ovat keränneet mobiilisovellusten avulla tietoja venäläisten sotilasosastojen liikkeistä, samalla kun tulosten analysointi on puhtaasti sotilastiedustelun vastuulla (Burke, 2022). Sitä vastoin ”kansalaisjournalistit” voidaan tiedustelun näkökulmasta mieltää myös tai ennen kaikkea analyytikoiksi.

2.3.5 Tiedustelu osana yritysten normaalia toimintaa

Tiedustelusta on viimeksi kuluneen kahdenkymmenen vuoden aikana tullut myös yritysten normaalia toimintaa esimerkiksi lentoyhtiöissä ja isoissa monikansallisissa yhtiöissä. Analyytikkojen työnkuvat vaihtelevat riskiarvioiden tekemisestä tilannekuvan ylläpitämiseen, mutta erilaisten ammatillisten seurojen ja foorumeiden yleistyminen osoittaa, että liiketoimintatiedustelu on ammattimaistumassa (Robson Morrow, 2022).

2.4 Ei-valtiollinen tiedustelu Ukrainan sodassa

Ukrainan sota avaa kiinnostavia ja ajankohtaisia näkymiä tiedustelumonopolin murtumiseen. Sota on tehnyt tunnetuksi muun muassa erilaisia avoimia lähteitä käyttäviä OSINT-yhteisöjä, samalla kun se on alleviivannut kaupallisten yritysten roolia tiedustelun kentällä.

2.4.1 OSINT-yhteisöjen tiedustelutoiminta

Pitkään aavisteltu Venäjän laajamittainen hyökkäys Ukrainaan alkoi torstaiaamuna 24. helmikuuta 2022. Hyökkäystä eivät seuranneet ainoastaan valtiolliset tiedustelupalvelut, vaan myös suuri joukko avointen lähteiden tiedusteluun erikoistuneita journalisteja ja kaupallisia tiedusteluyrityksiä. Tämän lisäksi useat vapaaehtoisista koostuvat OSINT-yhteisöt ovat seuranneet Ukrainan tilannetta vuoden 2014 Krimin anneksoinnista lähtien (Mighty Finland Podcast, 2022.)

Materiaalia Venäjän hyökkäyksestä ja sen valmistelusta löytyy runsaasti verkon avoimista lähteistä. Satelliittikuvien lisäksi katsottavissa on ollut kuvaa tieliikennekameroista, säätutka-asemien mittaustietoja sekä siviilien ja sotilaiden sosiaalisen median alustoilla julkaisemia valokuvia ja videotallenteita. Sotaa käydään ensimmäistä kertaa lähes reaaliaikaisesti sosiaalisessa mediassa. Avointen tiedustelulähteiden laajan saatavuuden myötä avointen lähteiden tiedustelusta on tullut myös osa kaikkien sotavoimien tiedustelun perustyötä. (HS, 2022.)

Esimerkkinä Ukrainan sotaa seuraavista OSINT-yhteisöistä toimii Ukrainan tilannekarttapalvelua, ”The War in Ukraine”, ylläpitävä suomalaisten reserviläisten ryhmä. Ukrainan tilannekarttapalvelusta on tullut lähde, jota eri mediat ovat lainanneet uutisointinsa tueksi. Karttapalvelun yhden perustajan, Emil Kastehelmen mukaan ryhmä on myös kyennyt ajoittain jopa tarkempaan analyysiin kuin valtiolliset tiedustelupalvelut: esimerkkinä useat totena uutisoidut ja myöhemmin vääriksi osoittautuneet tiedot Venäjän joukkojen jäämisestä motteihin hyökkäyksen aikana. (Mighty Finland Podcast, 2022).

Bellingcat-verkoston vapaaehtoiset taas varmistavat avointen lähteiden avulla valtiollisten toimijoiden Ukrainan sodasta raportoimien tietojen paikkansapitävyyden. Verkoston perustaja Eliot Higginsin mukaan Ukrainan sota on Bellingcatin tärkein projekti. Bellingcat kerää todistusaineistoa Ukrainan sodasta tuleville sukupolville, toimien Venäjän disinformaatiota vastaan. (Bellingcat, 2022.)

Higginsin mukaan verkoston vapaaehtoiset hyödyntävät työssään esimerkiksi Venäjällä ja Ukrainassa ahkerasti käytettyä Telegram-sovellusta. Useimmat sosiaalisen median sovellukset poistavat kuvien ja videoiden metatiedon, joka sisältää tiedon kuvansijaintikoordinaateista ja tallenteenottoajasta. Telegram toimii toisin, ja siksi sen julkaisut ovat arvokkaita geopaikantamisen ja tiedon varmistamisen näkökulmasta. Myös Tiktok on edesauttanut sodan tilannekuvan rakentamista, koska monet kuvaavat sodan tapahtumia klikkien toivossa. Twitter puolestaan toimii parhaiten verkoston omana viestintäkanavana. (Time, 2023.)

2.4.2 Kaupalliset yritykset

Myös kaupalliset tiedustelutoimijat ovat näytelleet merkittävää roolia Ukrainan sodassa. Etenkin Yhdysvaltojen asevoimien kanssa yhteistyötä tekevät tieto- ja sotateknologiaa sekä palveluita tarjoavat yritykset ovat rientäneet Ukrainan avuksi. Pentagon on

yrittänyt integroida jo pitkään olemassa olevia kaupallisia tuotteita ja teknologioita omakseen, mutta aikaisemmin instituutioiden välinen byrokratia ja teknologiayhtiöiden työntekijöiden protestit ovat asettuneet tavoitteen tielle. Ukrainassa tämä integraatio on tapahtumassa reaaliajassa, kun kaupalliset yritykset tarjoavat tuotteitaan asevoimien ja tiedustelupalveluiden käyttöön. (Guyer, 2022.)

Kaupallisten satelliittien määrä pysyi pitkään pienenä eikä niiden tuottamaa dataa ollut avoimesti saatavilla vielä Syyrian tai Afganistanin sotien aikaan. Sitä mukaa kun yksityisten ja kaupallisten satelliittien määrä on lisääntynyt, myös sensoriteknologia on edennyt nopein harppauksin. Etenkin Synthetic Aperture Radar eli SAR-kuvausteknologia, joka kykenee tuottamaan kuvaa pilviverhojen ja jopa kevyiden kattomateriaalien lävitse, on muodostunut tärkeäksi kuvaustiedustelun menetelmäksi. (Geospatial World, 2022.)

Venäjän hyökkäyksen alettua Ukrainan hallitus pyysi julkisesti Twitterissä, että kaupalliset satelliittiyritykset toimittaisivat ajantasaista SAR-dataa Ukrainan puolustusvoimille. (Mykhailo, 2022) Useampikin yritys kuten Capella Space, IceEye ja Satellogic on vastannut pyyntöön ja tarjoaa Ukrainan armeijalle geotiedustelun (GEOINT) tuottamaa tietoa. (Geospatial World, 2022.)

Kaupalliset satelliittiyritykset kykenevät nykyisin tuottamaan kuvaustiedustelumateriaalia, jonka tarkkuuteen ovat aikaisemmin pystyneet vain valtiolliset tiedustelupalvelut. Esimerkiksi Maxar WorldView tunnisti joukkohaudan sijainnin Mariupolin kaupungin ulkopuolella Itä-Ukrainassa (Clark, Stepanenko & Hird 2022). Yhtiö seurasi haudan asteittaista laajenemista useiden viikkojen ajan, kun Venäjän joukot kiihdyttivät taistelua kaupungin valtaamiseksi. Kuvaustiedustelun tiedoilla on tuettu myös humanitaarisia ponnisteluja, kun avustustoimijat ovat pyrkineet tunnistamaan turvallisia kulkuväyliä siviilien evakuoimiseksi. Myös sotarikoksia ja niiden tekijöitä on pyritty tunnistamaan kuvaustiedustelulla. (Ewin, 2022). Myös Bellingcat ostaa Planet Labs yrityksen tiedustelutuotteita. Planet Labsin satelliitit kykenevät tuottamaan liki valtiollisten tiedustelusatelliittien tasoista kuvaa mistä tahansa maankolkasta, muutaman päivän sisällä tuotteen tilaamisesta. (Bellingcat, 2021.)

Monet muutkin teknologiayritykset ovat tarjoutuneet auttamaan Ukrainaa. Elon Muskin johtama Starlink on antanut Ukrainan käyttöön satelliittiteknologiaan perustuvan verkkoyhteyden, josta on tullut kriittinen osa Ukrainan asevoimien johtamisjärjestelmää. (Shrimpton, 2022.)

Tiedustelun kannalta tärkeitä palveluita Ukrainan käyttöön ovat niin ikään toimittaneet big data –analytiikkaan erikoistunut Palantir Technologies, kasvojentunnistusteknologiaan erikoistunut Clearview AI sekä Microsoft ja Google. Esimerkiksi Microsoft on avustanut Ukrainan kyberhyökkäysten torjumisessa Krimin valtaamisesta lähtien, samalla kun Google on estänyt disinformaatiota tuottavia venäläismedioita hakutuloksistaan ja poistanut sumennukset Venäjän sotilaskohteiden päältä. (Guyer, 2022)

3 Johtopäätökset

Valtiollisen tiedustelumonopolin murtuminen ei ole tulevaisuutta, vaan nykyisyyttä. Monopolia kannatelleet pilarit ovat murtuneet tai murtumassa, ja tiedustelun kenttä on laajentunut suorastaan räjähdysmäisesti, kuten Ukrainan sotakin osoittaa.

Toisaalta valtiollisilla tiedustelupalveluilla on edelleen käytössä teknologioita ja kyvykkyyksiä, joita kaupalliset toimijat eivät vielä kykene tuottamaan. Monopoli on siis

osittain olemassa, mutta tilanteen voidaan olettaa muuttuvan jatkuvasti teknologisen kehityksen myötä.

Valtiollisen tiedustelumonopolin murtuminen sekä tiedustelun kentän moninaistuminen asettavat perinteiset tiedustelupalvelut uusien haasteiden eteen. Osa ei-valtiollisista toimijoista toimii viranomaisten intressien vastaisesti, mutta myös mahdollisuuksia on paljon, puhuttiinpa sitten tiedustelun ulkoistamisesta, uusista teknologioista tai yhteistyöstä. Ja kuten yllä on viitattu, yhteistyön tekeminen ei useissa tapauksissa ole pelkästään mahdollista, vaan myös välttämätöntä, mikäli tiedustelupalvelut haluavat hyötyä teknologisesta kehityksestä.

Olennainen kysymys perinteisten tiedustelupalveluiden kannalta on: kenen kanssa voidaan tehdä yhteistyötä ja millä ehdoilla? Asetelmaan liittyy haasteita, ei vähiten siksi että siinä missä tiedustelupalvelut pyrkivät yleensä salaamaan menetelmänsä, kyvykkyytensä ja lähteensä, pyrkivät esimerkiksi kansalaisjournalistit usein – joskaan eivät aina – kertomaan, millä menetelmillä ja millaisten lähteiden perusteella johtopäätöksiin on tultu. Miten siis sovittaa yhteen toisaalta läpinäkyvyys ja avoimuus sekä toisaalta oman toiminnan suojaaminen ja operaatioturvallisuus?

Ukrainan sota on nopeuttanut jo meneillään olevaa kehitystä, ja erilaisten kaupallisten tiedusteluyritysten, teknologiajättien sekä vapaaehtoistoimijoiden toimia seurataan nyt tarkasti. Sodan voi sanoa osittaneen konkreettisesti esimerkiksi avointen lähteiden tiedustelun, kaupallisten satelliittien ja kansalaistiedustelun arvon sekä toisaalta myös hämärtäneen entisestään rajaa siviilien ja sotaakäyvien tahojen välillä. Vaikutukset tulevat olemaan kauaskantoisia ja tulevaisuuden strategioita kirjoitetaan Ukrainan sodan pohjalta.

Lähteet

Betts, R. K. (1988). Policy-makers and intelligence analysts: Love, hate or indifference? *Intelligence and National Security*, *3*(1), 184–189. https://www.tandfonline.com/doi/pdf/10.1080/02684528808431934?needAccess=true

10 USC 467: Definitions. (ei pvm.). Haettu 18.11.2022 osoitteesta https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title10-section467&num=0&edition=prelim

Alibaba.com. (2022). Lidar&post-processing Software Available Flightweight Drone-mounted Lidar Surveying And Mapping System Uav 3d Mapping System—Buy Livox Avia Laser Scanner Surveying And Mapping System Uav 3d Mapping System,Lidar And Post-processing Software Available For Sale Lightweight Drone-mounted Lidar Surveying And Mapping System,Livox Avia Laser Scanner And Lightweight Drone-mounted Lidar Surveying And Mapping System Product on Alibaba.com. https://www.alibaba.com/product-detail/LIDAR-post-processing-software-available-flight-weight_1600409836394.html?spm=a2700.7724857.0.0.2cde3936CqUdrC

Althoff, M. (2016). Human Intelligence. Teoksessa Lowenthal, M. M. t., & Clark, R. M. (toim). *The five disciplines of intelligence collection*. CQ Press.

Airo, P. (14.9.2022). Ukrainan sodan tilannekartta kiinnostaa laajasti – suosio on

yllättänyt suomalaiset tekijätkin. Haettu 18.11.2022 osoitteesta https://reservilainen.fi/ukrainan-sodan-tilannekartta-kiinnostaa-laajasti-suosio-on-yllattanyt-suomalaiset-tekijatkin

Andrew, C. (2018). *The secret world: A history of intelligence*. Yale University Press.

Azulai, Y. (24.10.2019). "Black Cube Has Ethical Boundaries". Globes. https://en.globes.co.il/en/article-exposing-bribery-requires-trickery-such-as-impersonation-1001304648

Barger, D. G. (2005). Toward a Revolution in Intelligence Affairs. *RAND National Security Research Division*. https://apps.dtic.mil/sti/pdfs/ADA448571.pdf

Bellingcat. (23.3.2023). *About.* https://www.bellingcat.com/about/

Bellingcat. (21.9.2021). *Bellingcat Can Now Access Specialised Satellite Imagery. Tell Us Where We Should Look.* Haettu 18.11.2022 osoitteesta https://www.bellingcat.com/resources/2021/09/21/bellingcat-can-now-access-specialised-satellite-imagery-tell-us-where-we-should-look/

Bellingcat. (23.2.2022). *Documenting and Debunking Dubious Footage from Ukraine's Frontlines*. Haettu 20.11.2022 osoitteesta https://www.bellingcat.com/news/2022/02/23/documenting-and-debunking-dubious-footage-from-ukraines-frontlines/

Black Cube. (22.11.2022). *Black Cube*. https://www.blackcube.com/

Borowitz, M. (16.8.2022). War in Ukraine highlights importance of private satellite companies. *The Conversation*. Haettu 1.4.2023 osoitteesta https://theconversation.com/war-in-ukraine-highlights-the-growing-strategic-importance-of-private-satellite-companies-especially-in-times-of-conflict-188425

Burke, P. (2022). The Issues in the Collection, Verification, and Actionability of Citizen-derived and Crowdsources Intelligence during the Russian Invasion of Ukraine, 2022. *Strategic Panorama*, 94-103. https://doi.org/10.53679/2616-9460.special-issue.2022.09

Clark, M., Stepanenko, K., & Hird, K. (10.4.2022). Russian Offensive Campaign Assessment, April 10. *Institute for the Study of War.* Haettu 19.11.2022 osoitteesta https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-april-10

European Commission. (2.5.2022). Open-source intelligence. Haettu 18.11.2022 osoitteesta https://data.europa.eu/en/publications/datastories/open-source-intelligence

Ewing, T. (21.2.2022). The Real Power of Intelligence 'Auxiliaries'. *The Cipher Brief*. Haettu 18.11.2022 osoitteesta https://www.thecipherbrief.com/the-real-power-of-intelligence-auxiliaries

Gentry, J. A. (2016). Toward a Theory of Non-State Actors' Intelligence. *Intelligence and national security, 31*(4), 465-489. https://doi.org/10.1080/02684527.2015.1062320

Geospatial World. (2022). GeoInt, OSINT Comes Off Age For Near Real Time Coverage

of Ukraine. Haettu 18.11.2022 osoitteesta https://www.geospatial-world.net/blogs/geoint-osint-comes-off-age-of-ukraine-conflict/

Guardian. (7.12.2020). It's a free-for-all': how hi-tech spyware ends up in the hands of Mexico's cartels. *The Guardian*. https://www.theguardian.com/world/2020/dec/07/mexico-cartels-drugs-spying-corruption

Guo, B., Wang, Z., Yu, Z., Wang, Y., Yen, N. Y., Huang, R., & Zhou, X. (2015). Mobile Crowd Sensing and Computing: The Review of an Emerging Human-Powered Sensing Paradigm. *ACM Computing Surveys*, 48(1), 7:1-7:31. https://doi.org/10.1145/2794400

Guyer, J. (21.9.2022). The West is testing out a lot of shiny new military tech in Ukraine. Haettu 19.11.2022 osoitteesta https://www.vox.com/2022/9/21/23356800/us-testing-tech-ukraine-russia-war

Higgins, E. (2022). *The online sleuths 'We are Bellingcat' Solving Global*. Bloombury.

Hirshorn, Y. (9.6.2018). Inside Black Cube - The "Mossad" of the Business World. *Forbes Israel*. Arkistoitu 3.10.2021: https://web.archive.org/web/20211003153224/https:/forbes.co.il/e/behind-closed-doors-first-peek-into-the-israeli-company-that-captivates-global-interest/. Haettu 19.11.2022.

France24. (2022). How Bellingcat became Russia's 'biggest nightmare'. (7.9.2022). *France24*. Haettu 20.11.2022 osoitteesta https://www.france24.com/en/live-news/20220907-how-bellingcat-became-russia-s-biggest-nightmare

HS. (2022) Ukrainan sota. Sodan etenemistä seurataan tiiviisti Helsingin Pukinmäen "tilannehuoneessa": Suomalaisryhmä teki tarkan kartan, jota sotilasasiantuntijatkin kommentoivat. (6.3.2022). *Helsingin Sanomat*. Haettu 18.11.2022 osoitteesta https://www.hs.fi/sunnuntai/art-2000008651005.html

Iceye a (18.8.2022). ICEYE Signs Contract to Provide Government of Ukraine with Access to Its SAR Satellite Constellation. *Iceye.* https://www.iceye.com/press/press-releases/iceye-signs-contract-to-provide-government-of-ukraine-with-access-to-its-sar-satellite-constellation

Iceye b (20.11.2022). *Iceye*. https://www.iceye.com/

Janes (20.11.2022). *About Janes*. https://www.janes.com/about-janes/what-we-do

Jardines, E. A. (2016). Open Source Intelligence. Teoksessa Lowenthal, M. M. t., & Clark, R. M. (toim). *The five disciplines of intelligence collection*. CQ Press.

Jungherr A. Rivero Rodríguez Gonzalo & Gayo-Avello D. (2020). *Retooling politics how digital media are shaping democracy*. Cambridge University Press.

Kari, M. J. (2020). Tiedustelu yliopistollisena oppialana – myös Suomessa? Teoksessa T. Koivula (toim.) *Suomalaisen tiedustelukulttuurin jäljillä* (s. 105-123). Maanpuolustuskorkeakoulu, Sotataidon laitos.

MacLeod, D. T. (2009). Leveraging Academia to Improve NGO Driven Intelligence. *Journal of Conflict Studies*, 29.

Matovski, A. (2020). Strategic Intelligence and International Crisis Behavior. *Security*

studies, 29(5), 964-990. https://doi.org/10.1080/09636412.2020.1859128

McDowell, D. (2009). *Strategic intelligence: A handbook for practitioners, managers, and users (Rev. ed.)*. Scarecrow Press.

Megiddo, G. (22.8.2019). Israel Hired Black Cube, Allowing Spy Firm to Operate Out of Military Intel Base. *Haaretz*. Haettu 19.11.2022 osoitteesta https://www.haaretz.com/israel-news/2019-08-22/ty-article/.premium/for-black-cube-israeli-government-was-both-customer-and-target/0000017f-f2f0-d8a1-a5ff-f2fa360b0000

Meier, B. (2021). *Spooked: The secret rise of private spies*. Sceptre.

Mighty Finland Podcast: OSINT ja Ukrainan sodan alku - Emil Kastehelmi & Eerik Matero Apple Podcasts -palvelussa. (ei pvm.). Haettu 19.11.2022 osoitteesta https://podcasts.apple.com/fi/podcast/osint-ja-ukrainan-sodan-alku-emil-kastehelmi-eerik-matero/id1507675257?i=1000581548029&l=fi

Moore, R. (30.11.2021). *C's speech to the International Institute for Strategic Studies.* https://www.gov.uk/government/speeches/cs-speech-to-the-international-institute-for-strategic-studies

Murdock, D. & Clark, R.M. (2016). Geospatial Intelligence. Teoksessa Lowenthal, M. M. t., & Clark, R. M. (toim.). *The five disciplines of intelligence collection*. CQ Press.

Mykhailo F. (1.3.2022). @eos_da and @maxpolyakov appeal to the global remote sensing firms and organizations to provide real-time SAR data to support the Armed Forces of Ukraine with actionable intelligence. https://t.co/DzfNze3K3r [Tweet]. Haettu 18.11.2022 osoitteesta https://twitter.com/FedorovMykhailo/status/1498664494301650950

NGA Growing in Acceptance of Satellite Imagery Startups—Via Satellite -. (28.9.2016). Haettu 19.11.2022 osoitteesta https://www.satellitetoday.com/innovation/2016/09/28/nga-growing-acceptance-satellite-imagery-startups

Nolte, W. N. (2016). Signals Intelligence. Teoksessa Lowenthal, M. M. t., & Clark, R. M. (toim). *The five disciplines of intelligence collection*. CQ Press.

Orbis Business Intelligence (20.11.2022). *About Orbis*. https://orbisbi.com/about-orbis/

Peltonen, E. (16.4.2018). Mitä tarkoittaa tiedon ubiikki käsittely? - Tietysti.fi. https://www.aka.fi/tietysti/kysy-tieteesta/mita-tarkoittaa-tiedon-ubiikki-kasittely/

Porvali, M. (2022). *Tiedustelun näkymätön historia: Antiikista maailmansotiin*. Otava.

Rathmell, A. (2002). Towards postmodern intelligence. *Intelligence and National Security*, 17(3), 87–104. https://doi.org/10.1080/02684520412331306560

Reagan Foundation. (2022). Countering Foreign Information: Developing a Whole of Society Approach to build Resilience. A panel discussion the Reagan Foundation's Center for Freedom and Democracy. https://youtu.be/0E20OfKk_aY

Robson Morrow, M. (2022). Private sector intelligence: on the long path of professionalization. *Intelligence and National Security*, 37:3, 402-420, DOI: 10.1080/02684527.2022.2029099

Shrimpton, B. (18.10.2022). Starlink satellite support of Ukraine shows value of government–private sector cooperation. Haettu 19.11.2022 osoitteesta https://www.aspistrategist.org.au/starlink-satellite-support-of-ukraine-shows-value-of-government-private-sector-cooperation/

Teppati Losè, L., Spreafico, A., Chiabrando, F., & Giulio Tonolo, F. (2022). Apple LiDAR Sensor for 3D Surveying: Tests and Results in the Cultural Heritage Domain. *Remote Sensing*, 14(17), Article 17. https://doi.org/10.3390/rs14174157

Time. (2023). Bellingcat's Eliot Higgins Explains Why Ukraine Is Winning the Information War. Haettu 20.11.2022 osoitteesta https://time.com/6155869/bellingcat-eliot-higgins-ukraine-open-source-intelligence/

U.S. GEOINT Is Clear Driver in Ukrainian Defense. (ei pvm). Haettu 18.11.2022 osoitteesta https://www.afcea.org/signal-media/intelligence/us-geoint-clear-driver-ukrainian-defense

Weinbaum, C., Berner, S., McClintock, B. (2017). SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain. *RAND Corporation*. https://www.rand.org/pubs/perspectives/PE273.html

West, N. (2015). *Historical Dictionary of International Intelligence: Vol. Second edition*. Rowman & Littlefield Publishers.

Whitford, T., & Prunckun, H. (2017). Discreet, not covert: Reflections on teaching intelligence analysis in a non-government setting. *Salus Journal*, 5(1), 48-61. https://search-informit-com-au.ezproxy.csu.edu.au/documentSummary;dn=667617804406903;res=IELHSS

Zwitter, A. (2016). *Humanitarian Intelligence: A Practitioner's Guide to Crisis Analysis and Project Design*. Rowman & Littlefield.

Liite 1. Postmodernismin ydinteemat

Taulukko 1 Postmodernismin ydinteemat (Rathmell, 2002, s. 95–96)

Ydinteema	Ydinteema
Suurien narratiivien loppu; ei yritetä löytää kaiken selittäviä yhteiskunnallisia teorioita, joilla voitaisiin selittää sosiaalisia aktiviteettejä. Postmodernismi korvaa kaiken selittävän teorian vaihtoehtoisilla narratiiveilla ja näkökulman pirstaleisella maailmankatsomuksella. Lineaarisuuden ja progressiivisten historiallisten muutosten sijaan postmodernismi tarjoaa tilalle epälineaarisuutta, rekursiivisuutta ja kaaosta.	**Absoluuttisten totuuksien etsimisen lopettaminen;** tunnistetaan tutkijoiden rooli toimijana ja osallistujana. Postmodernismi ei pyri tekemään havaintojen yhtenäisestä todellisuudesta, vaan tulkitsee sosiaalisia ja kielellisiä rakenteita, jotka vaikuttavat tiedon tuottamiseen.
Puuttuvat keskustat ja epävarmat identiteetit; perustavanlaatuisen binäärisen ajattelun murtuminen. Postmodernismi purkaa sosiaalis-kielellisiä rakennelmia, jotka vahvistavat binäärisiä vastakohtia kuten mies/nainen, ihminen/kone, paikallinen/globaali. Postmodernit teoriat heijastavat väitetysti nykyistä yhteiskuntaa, jossa teknologiset, sosiaaliset ja taloudelliset muutokset hajottavat binäärisiä vastakohtia.	**Liikkuvat rajanvedot;** kilpailevien teorioiden (kuten poliittis-taloudellis-teknologinen vs. deterministis-sosiaalinen konstruktivismi tai liberalismi vs. Marxismi) korvaaminen joustavilla, monipuolisilla selityksillä. Modernismin vahvat raja-aidat ovat muuttuneet huokoisiksi, läpäistävissä oleviksi ja hämärtyneiksi raja-aidoiksi tai rajoiksi valtioiden, kulttuurien ja yritysten välillä.
Osaamistalous; tuotannon hiipuminen jälkiteollisissa yhteiskunnissa, tietotyöläisen nousu. Tällä kehityksellä on kauaskantoisia vaikutuksia yhteiskunnan "järjestäytymättömyyteen": hierarkkiset rakenteet korvautuvat verkoilla ja yleiset mediat vuorovaikutteisilla, personoiduilla tiedotusvälineillä. Lojaalius yrityksiä kohtaa loppuu ja itsenäisen osaamistyöntekijän merkitys korostuu.	

Liite 1. Postmodernin tiedustelun ydinteemat

Taulukko 2 Postmodernin tiedustelun ydinteemat (Rathmell, 2002, s. 97–98)

Ydinteema	Ydinteemat
Kohteiden, roolien ja tehtävien pirstaloituminen; Neuvostoliiton hajoamisen jälkeen tiedustelupalveluiden on ymmärrettävä useita, päällekkäisiä ja usein vastakkaisia narratiiveja. Postmodernit tiedustelupalvelut ovat alkaneet löytää aikaisemmin marginaalissa olleita kohteita. Palveluiden on myös ymmärrettävä maailmaa, joka vaikuttaa kaoottiselta ja kehitystä, jossa on ominaisuuksia ei-lineaarisesta, dynaamisesta järjestelmästä.	**Arvoituksia ei palapelejä**; kylmän sodan aikainen tiedustelu tiesi ongelman ja pystyi kuvittelemaan objektiivisen todellisuuden, jota se pyrki ymmärtämään. Nykyisin tiedustelu ei tiedä, onko olemassa yhtä objektiivista todellisuutta, jota se yrittää saada kiinni.
Identiteetti; mikrotasolla tiedusteluyhteisöä, kuten muutakin yhteiskuntaa, sekä sen identiteettiä haastetaan monesta suunnasta. Teknologian kyllästämässä tiedustelun maailmassa ihmisen ja laitteen välinen dikotomia on uhattuna automaattisten järjestelmien ja kyborgikäsitteen nousun myötä. Makrotasolla tiedustelupalvelujen identiteetit ovat uhattuina; enää ei ole selvää, kenelle tai ketä vastaan tiedustelutuotetta tehdään. On epäselvää, mille hallinnon organisaatiolle, mille valtiolle, mille ylikansalliselle organisaatiolle tai yritykselle tuote on tarkoitettu.	**Häilyvät raja-aidat**; kylmän sodan aikaiset tarkat raja-aidat ovat nykyään häilyviä ja ne voidaan läpäistä. Horisontaaliset tietoyhteisöt kilpailevat vertikaalisten kansallisten rakennelmien kanssa tietämyksen ja tiedustelutuotteen tuottamisessa. Lojaaliuden ja ammattimaisen osaamisen rajat ovat murtumassa. Yksityiselle sektorille tulee aiemmin luottamukselliseksi luokiteltua teknologiaa ja ammattiosaamista, samalla kun valmiiden kaupallisten teknologioiden ja osaamisen lisääntyvä käyttö korostaa käynnissä olevaa muutosta.
Tiedustelutehtaan loppu; klassinen konsepti tiedustelutehtaasta on vanhentunut. Osaamistalous, joka hyödyntää teknologiaa ja sosiaalista muutosta, muuttaa tiedusteluliiketoimintaa ja palveluita, samalla kun se muuttaa kaupankäyntiä, hallintoa ja asevoimia.	

DISRUPTIIVISTEN TEKNOLOGIOIDEN VAIKUTUS TIEDUSTELUUN

Pasi Hario, Elisa Norvanto, Niko Reinvall, Jussi Segler

1 Johdanto

Tämä raportti tarkastelee disruptiivisten teknologioiden vaikutuksia tiedustelutoimintaan. Disruptiivisilla teknologioilla viitataan uusiin tietoteknisiin tai teknologisiin sovelluksiin, jotka muokkaavat tai joilla on potentiaalia muokata yksilöiden, yhteisöjen ja toimialojen toimintaa systeemitasolla. Tiedustelutoimintaa käsitellään klassisen ohjaukseen, keräykseen, käsittelyyn ja jakamiseen jakautuvan tiedustelukehän kautta. Luvussa 2 käsitellään disruptiivisia teknologioita ja tiedustelua, ja luvussa 3 esitellään neljä disruptiivista teknologiaa: koneoppiminen, lohkoketjut, kvanttiteknologia ja esineiden internet. Aiheiden valinta perustuu Hershkovitzin (2022) listaukseen tiedustelun näkökulmasta kiinnostavimmista teknologioista. Luvussa 4 esitetään johtopäätökset edellisistä johdanto- ja käsittelyluvuista. Raportin lähdeaineisto on kerätty julkisista, avoimista lähteistä.

2 Käsitteitä

2.1 Tiedustelukehä

Tiedustelun tehtävä on tuottaa tietoa vastustajasta ja olosuhteista päätöksenteon tueksi. Tiedustelutoiminnan kuvauksista on useita muunnoksia. Suurin osa niistä on kuitenkin kuvattu tiedustelukehiksi, joiden välivaiheiden lukumäärät vaihtelevat ja jotka ovat iteratiivisessa vuorovaikutuksessa keskenään. Esimerkiksi monissa tiedusteluvaiheiden kuvauksissa datan keruun jälkeen tietoa prosessoidaan, eli luokitellaan ja järjestellään, ja vasta sitten analysoidaan, eli liitetään eri konteksteihin ja tehdään siitä arvioita. Toisissa kehissä taas prosessointi ja analysointi on yhdistetty keräysvaiheeksi. Eroja kehien välillä on myös esimerkiksi keräys- tai analyysivaiheen jälkeen tiedustelutiedon toimittamisessa asiakkaalle. Osa jakaa vaiheen palaute- ja jakamisvaiheeseen, ja osassa kehistä ne ovat yhdistetty pelkän jakamisvaiheen alle. (Lowenthal & Clark, 2016; Smith & Brooks, 2013.)

Ohjaus sisältää asiakkaan tietopyynnön vastaanottamisen, sen pohjalta tehdyn tiedonkeruusuunnitelman ja toimeksiannon aihealueen taustatutkimuksen ymmärryksen saavuttamiseksi toimeksiannosta. Keräysvaiheessa dataa kerätään eri keräyslajien avulla noudattaen ja tarvittaessa muokaten ohjausvaiheen tiedonkeruusuunnitelmaa. Käsittelyvaiheessa data luokitellaan ja järjestellään kokonaisuuksiksi eli informaatioksi. Tämän jälkeen informaatio analysoidaan testaten hypoteeseja sekä laatien arvioita tutkittavan kohteen nykytilasta ja kehityskuluista. Ohjausvaiheessa tuotettu tietämys tai ymmärrys muotoillaan ymmärrettävään ja vaikuttavaan muotoon sekä esitetään asiakkaalle tavoitteena tukea hänen päätöksentekoaan. (Smith & Brooks, 2103; McDowell, 2009.)

2.2 Disruptiiviset teknologiat

Bowerin ja Christensenin voidaan katsoa luoneen käsitteen ‘disruptiivinen teknologia’. Teoksessaan *”Disruptive technologies: catching the wave”* (1995) he kuvasivat, miten eri alojen suuret markkinajohtajat epäonnistuivat uusien teknologioiden hyödyntämisessä kehittäessään omaa tuotettaan yhä paremmaksi, jättäen pienet uudet innovaatiot omalla alallaan huomiotta. Näistä pienistä uutuuksista nousi kuitenkin alansa johtavia toimijoita markkinajohtajien kustannuksella.[1] Myöhemmin Christensen (2003) laajensi tätä käsitettä ajatuksella, että teknologia itsessään ei ole disruptoiva. Vasta kun teknologiaa hyödynnetään liiketoiminnassa, tulee siitä disruptoiva. Tällöin itse liiketoimintamalli on disruptoiva, kuten Gobble (2016) asian tiivistää. Christensenin näkemys on saanut myös kritiikkiä liian kapeasta katsantokannasta. Disruptiivisia teknologiota eivät ole vain uudet tuotteet ja sovellukset, vaan ne ovat myös tapoja laajentaa olemassa olevia markkinoita tai uusien toiminnallisuuksien kehittämistä (Utterback, 2005). Teknologinen kehitys kiihtyy (kts. Singh, 2021). Uudet teknologiat, joilla on potentiaalia luoda täysin uudenlaisia tapoja tyydyttää kuluttajien tarpeita, luoda uusia markkinoita tai synnyttää uudenlaisia liiketoimintamalleja, ovat monelle yritykselle mielenkiinnon kohteita. Sitä ne ovat myös tiedusteluyhteisölle (Katz, 2020).

Tiedusteluorganisaatiot käyttävät suuren osan resursseistaan vaikeasti saatavilla olevan tiedon keräämiseen. Näin ollen tiedusteluyhteisön toiminnan näkökulmasta mielenkiintoisia disruptiivisia teknologioita ovat teknologiat, jotka voivat helpottaa datan keräämistä, varastointia, prosessointia ja analyysia.

Hershkovitzin (2022) mukaan esineiden internet (IoT), 5G, Big data-analytiikka, tekoäly, lohkoketju ja kvanttilaskenta voivat tehostaa tiedustelutoimintaa.[2] Hyödyntämällä näitä teknologioita, tiedusteluorganisaatioiden resursseja vapautuu sinne, mistä ihmisen kognitiivisista kyvyistä on eniten hyötyä: tulkintaan, merkitysten löytämiseen ja päätöksentekoon.

3 Disruptiiviset teknologiat ja tiedustelu

Tässä luvussa käsitellään disruptiivisia teknologioita ja niiden mahdollisia ja todennäköisiä vaikutuksia tiedustelutoimintaan. Teknologioiden hyödyntämistä tarkastellaan tiedustelukehän eri vaiheissa.

---

[1] Esimerkiksi IBM jäi kilpailijiostaan jälkeen minitietokoneiden markkinoissa. Digital Entertainmentin ei puolestaan päässyt kannettavien tietokoneiden markkinoiden kyytiin hallitessaan minitietokonemarkkinaa. Kodak jäi jälkeen valokuvauksen digitalisoituessa. Blockbuster inc. taas jäi suoratoistopalvelujen jalkoihin. (Thangavelu, 2020.) Uber on esimerkki lähihistorian disruptiosta (Muller, 2020.)

[2] Hershkovitzin (2022) listaus on kattava otos tiedusteluyhteisön toimintaan vaikuttavista teknologioista. Disruptiivisia teknologioita on toki muitakin. Esimerkiksi NATO (2022), Yhdysvaltain puolustusministeriö (Vergun, 2022) ja National Intelligence Council (2008). Myös Gartnerin (Davies, 2022) vuosittain julkaisemassa “Hype cycle of emerging tech, 2022”-katsauksessa luetellaan useita eri tekoälyn ja lohkoketjun sovelluksia, jotka ovat tällä hetkellä potentiaalisesti disruptoivia.

3.1 Koneoppiminen (Machine Learning)

OECD (2020) on nimennyt tekoälyn yhdeksi merkittävimmäksi megatrendiksi osana yhteiskunnan digitalisoitumista. Tekoäly on laaja kattokäsite. Tekoälyksi voidaan kutsua konetta, joka on ohjelmoitu jäljittelemään ihmiselle (ja joillekin eläimille) tyypillistä ajattelua imitoivaa toimintaa yhdistelemällä dataa huipputekniikkaan (IBM, 2020; NATO, 2020). Tavoitteena on koneen automatisoitu ja jopa autonominen kyky tehdä päätelmiä ja päätöksiä, suunnitella, oppia tai peräti luoda uutta (Boucher, 2020).

Koneoppiminen on tekoälyn alakäsite. Sen mukaisesti kone on ohjelmoitu oppimaan tunnistamalla kaavoja ja säännönmukaisuuksia suurista datamassoista. Säännönmukaisuuksista kone tekee tulkintoja esimerkiksi ennakoiden tulevia kehityskulkuja tai kartoittaen riskejä. (OECD, 2020; SAS, 2021) Koneoppimisen mahdollistavat muun muassa tietomäärien kasvu ja saatavuus, tehokkaammat algoritmit, kyky prosessoida luonnollisia kieliä (engl. natural language processing) ja tietokoneiden prosessoritehon kasvu. Tekoäly ja koneoppiminen sen alakäsitteenä muuttavat myös tiedustelun toimintaympäristöä ja katalysoivat tiedusteluprosessin kaikkia vaiheita, kuitenkin voimakkaimmin keräys- ja käsittelyvaiheita (Katz, 2020). Koneoppiminen nopeuttaa tiedon prosessointia ja analyysia sekä vähentää erilaisten kognitiivisten vinoumien riskiä.

Tiedustelutehtävä lähtee liikkeelle yleensä asiakkaan tietopyynnöstä ja sen pohjalta tehtävästä keräyssuunnitelmasta. Ihminen tarvitaan edelleen antamaan koneelle toimeksiannon ensisyöte. Laajoja avoimia ja suljettuja tietomassoja rutiininomaisesti seulova sovellus saattaa kuitenkin löytää indikaattoreita, joiden pohjalta päätöksentekijät tai kone itse voi tarkentaa toimeksiantoa. Suunnittelussa voidaan jo nyt käyttää tekoälypohjaisia ohjelmia, jotka luovat osittain tai kokonaan vaikkapa keräyssuunnitelman (McDowell, 2009). Koneoppimista voidaan myös soveltaa tutkittaessa ja analysoitaessa tehtyjen keräyssuunnitelmien suhdetta tiedusteluprosessin lopputuloksiin. Tavoitteena voisi olla valjastaa tekoäly luomaan aineiston pohjalta toimivia ja tavoitteellisia tiedusteluprosesseja.

Kaupallisia koneoppimisen sovelluksia käytetään erityisesti avointen lähteiden valtavien datavirtojen keräämisessä. Koneoppimisessa tekoäly kykenee myös itsenäisesti täsmentämään keräysehtoja ja hakuparametrejä perustuen kerättyyn ja käsiteltyyn tietoon. Koneoppimisen tehokkaampi tietomassojen kerääminen pätee myös muihin tiedustelulähteisiin, kuten geotiedusteluun ja sen alla erityisesti kuvatiedusteluun. (Katz, 2020.)

Digitalisaation myötä tiedustelu kykenee keräämään valtavia tietomassoja, joita koneoppimisella voidaan käsitellä nopeasti ja tehokkaasti. Eri tietomassoihin ja tiedustelulähteisiin kytketty kone voi myös hetkessä tutkia johtolankoja, joita ei ole ihmisaistein mahdollista tai taloudellista lähteä keräämään tai myöhemmin käsittelemään. Tällaiset massat ovat tyypillisimpiä mittaus- ja tunnusmerkkitiedustelu-, geotiedustelu- ja signaalitiedustelulähteille. Geotiedustelun alla kuvaustiedustelussa esimerkiksi konenäkö (engl. computer vision) auttaa kuvien tunnistamisessa ja luokittelussa, ja sen avulla päästään kiinni kuvan ominaisuuksiin, joita ihmissilmän on mahdotonta havaita. Signaalitiedusteluun kuuluvassa viestitiedustelussa (engl. communication intelligence) taas luonnollisten kielten käsittelyprosessointi mahdollistaa sen, ettei ihmisten välisen kielellisen kanssakäymisen käsittelyyn tarvita ihmiskorvaa. (Katz, 2020.)

Tekoälypohjaisen koneoppimisen käyttö saattaa säästää tiedusteluprosessin inhimillisiltä kognitiivisilta virhetoiminnoilta, kuten vahvistusharhalta tai ryhmäajattelulta.

Konemielen keräys ja käsittelyalgoritmit eivät vääristy sosiaalisesta paineesta tai ennakkoluuloista. Viimeaikaiset esimerkit ovat kuitenkin paljastaneet, että tekoälyä ohjaavat algoritmit on syytä valita huolella (BBC, 2018). Algoritmit ja data vaikuttavat siihen, miten tekoäly tulkitsee ja analysoi dataa.

Silti, etenkin prosessointivaiheessa oppiva kone kykenee luokittelemaan ja lajittelemaan valtavia tietomassoja. Lisäksi tekoälyn suodattaessa tietoa jää ihmismieleltä enemmän aikaa keskittyä joko luovuutta vaativiin analyyttisiin tehtäviin tai ohjausvaiheen kanssakäymiseen toimeksiantajan kanssa. Kiinnostavaa on, että koneoppimisen myötä tekoäly voi tehdä käsittelyn perusteella kalibrointia sekä suunnittelu- että keräysvaiheeseen.

Jakeluvaiheessa tekoäly mahdollistaa automaattisten sisältöjen tuottamisen keräysvaiheen perusteella. Koneoppimisen kautta sisältöjä voi räätälöidä päätöksentekijöiden palautteen perusteella vastaamaan päätöksenteon tarpeita. Jos eri tiedusteluorganisaatiot tai valtiot tekevät yhteistyötä, voivat sovellukset myös jakaa reaaliaikaisesti tietoa toisillensa täydentäen keräys- ja käsittelyvaiheita. Tämä vaatii kuitenkin äärimmilleen vietyä valtioiden välistä yhteistyötä (esimerkiksi Five Eyes -tiedusteluyhteisö). (ODNI, 2019.)

3.2 Lohkoketjut (Blockchains)

3.2.1 Lohkoketjuteknologian sovellutukset ja regulaatio

Lohkoketju on digitaalinen tietokanta, rekisteri tai tilikirja, joka sisältää informaatiota, ja jota voidaan käyttää samanaikaisesti ja jakaa laajasti, hajautetussa ja julkisesti saatavilla olevassa verkossa. (Merriam-Webster, 2022) Stenfors (2019) kuvaa lohkoketjujen perusominaisuudet seuraavasti:

> Hajautettu tietoarkkitehtuuri, joka on peukaloimaton, yhteistyöhön kannustava, hajautettu ja välikädetön. Nämä ominaisuudet aikaansaavat tehokkaammat transaktiot ja mahdollistavat ennestään tuntemattomien osapuolten luotettavan toiminnan. Ne ovat lohkoketjujen ydin. (Stenfors, 2019, s. 71–72)

Lohkoketjuteknologia tulee mahdollistamaan sellaisten sovellusten ja innovaatioiden tuottamisen, joiden vaikutus voi olla huomattavan merkittävä. Se on teknologia, jolla on potentiaalia lisätä avoimuutta yhteiskunnassamme. Lansiti ja Lakhani (2017) mukaan lohkoketjuteknologia ei ole ainoastaan disruptoiva teknologia vaan fundamentaali teknologia, joka leviää hitaasti ja hallitusti eri aloille.

Lohkoketjun tunnetuin, ja myös ensimmäinen sovelluskohde on ollut kryptovaluutta Bitcoin (mm. Foroglou & Tsilidou, 2015; Xu ym., 2019). Lohkoketjuun perustuvien valuuttojen määrä on lisääntynyt, eikä niiden määrästä ole tarkkaa tietoa. Myös erilaisia valtioiden takaamia virtuaalisia valuuttoja on jo käytössä. Virtuaalinen valuutta on otettu käyttöön esimerkiksi Jamaikalla, ja Kiinassa virtuaalinen valuutta on pilottikäytössä (Bank of Jamaica, 2021; Peoples bank of China, 2022). Kryptovaluuttojen ja keskuspankkien digitaaliset valuutat voivat muuttaa tapaa, jolla vaihdantaa tehdään tulevaisuudessa.

Kryptovaluutat ovat selvästi tunnetuin lohkoketjuteknologian käyttökohde tällä hetkellä, mutta ei suinkaan ainoa. Lohkoketjulla on myös paljon muita erilaisia sovelluskohteita (mm. Xu ym., 2019; Mettler, 2016; Hsiao ym., 2018) ja aloja digitaalisen valuutan ja finanssisektorin lisäksi. Muun muassa terveydenhuolto, toimitusketjujen hallinta,

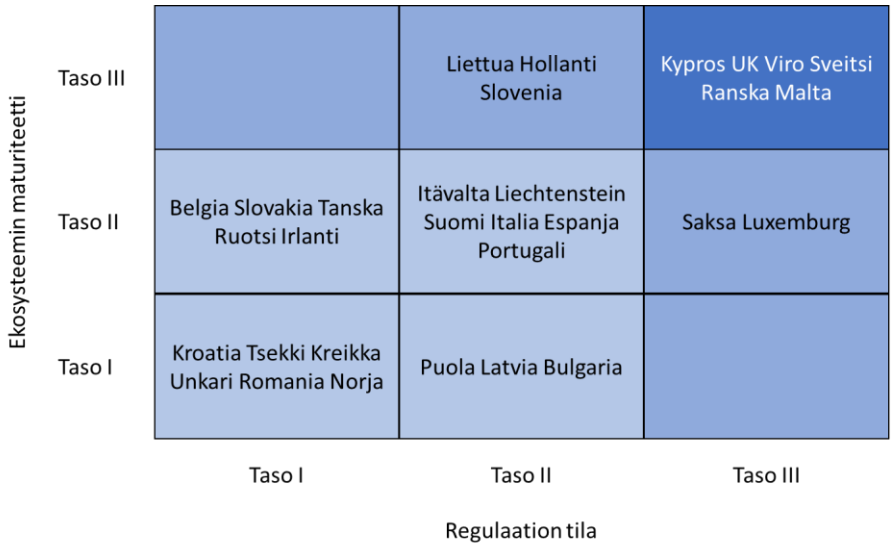
julkishallinto, tekijänoikeus, älykkäät sopimukset ja äänestäminen ovat olleet tutkijoiden mielenkiinnon kohteena. Myös signaalitiedusteluun liittyvää vertaisverkkoa, lohkoketjua ja koneoppimista hyödyntävää radiosignaalin salaussovellusta on tutkittu (Akter ym., 2021).

Myös lohkoketjuihin liittyvä lainsäädäntö on kehittyvä alue uusien sovelluksien kehittämisen myötä. Esimerkiksi julkisissa lohkoketjusovelluksissa datan avoimuus ja yleinen tietosuoja-asetus (engl. General data protection regulation, GDPR) ovat ilmeisessä ristiriidassa. Esimerkiksi GDPR-asetuksen artikla 17 (Euroopan parlamentti ja neuvosto, 2016) “oikeus unohtua” ei onnistu koska lohkoketju on muuttumaton ja siten transaktioita ei voida häivyttää siitä. (Haque, ym. 2021.) Myös Tatar, Gokce ja Nussbaum (2020) tutkivat lohkoketjujen ja GDPR:n välistä ristiriitaa ja argumentoivat, että Euroopan ei ole mahdollista välttyä lohkoketjuja käyttäviltä applikaatioilta ja standardeilta ristiriidasta huolimatta. Kaikki lohkoketjusovelluksia ei myöskään voida tehdä GDPR:n vaatimusten mukaisesti.

Yleisesti voisi jopa argumentoida, että valtioiden tahto hallita (keskitetty hallinta) on koetuksella lohkoketjuihin (hajautettu hallinta) perustuvien sovellusten ja käytänteiden lisääntyessä yhteiskunnassa. Esimerkiksi Venäjän presidentti Vladimir Putin puheessaan Valdai clubilla 27.10.2022 (Putin, 2022) kuvasi avoimen lohkoketjutyylisen talousalustan tarpeen. Tämä tukee Venäjän pyrkimyksiä kehittää omaa digitaalista valuuttaansa, joskin valuutta itsessään perustuu valtion takaamaan järjestelmään (Bank of Russia, 2020) ja Venäjällä on vahva intressi vähentää riippuvuuttaan Yhdysvaltain dollarista (Shagina, 2022). Teknologia helpottaa myös rikollista toimintaa (Suitto, 2019), joskaan ei aukottomasti (esim. Salisu ym., 2022).

Vuonna 2018 perustetun Euroopan unionin yhteistyöfoorumin EU Blockchain Observatory & Forumin julkaisemassa raportissa (EU Blockchain Observatory and Forum, 2022) arvioitiin muun muassa eri Euroopan maiden tämänhetkistä maturiteettia lohkoketjun reguloinnissa ja lohkoketjuekosekosysteemien kehittyneisyydessä kolmella alueella: liiketoiminta, akatemia ja yhteisöt (KUVIO 1). Ala kehittyy jatkuvasti ja onkin todennäköistä, että kuvion vasemman alalaidan valtioiden ekosysteemit ja regulaatiot kehittyvät ajan kuluessa.

Lohkoketju on mielenkiintoinen nouseva teknologia. Tästä ovat esimerkkeinä Eurooppaan perustettu lohkoketjun seurantaan keskittyvä foorumi (EU Blockchain observatory & forum), Yhdysvaltain kotimaan turvallisuusviraston lohkoketjukiinnostus (Department of homeland security, 2019) ja Kiinan ja Venäjän digitaaliset valuutat sekä Ukrainan pyrkimys digitalisoida oma hallintonsa kansalaispalveluksi (Ministry and committee digital transformation Ukraine, 2022).



KUVIO 1 Eri Euroopan maiden lohkoketjun regulaation ja ekosysteemin maturiteetti. Mukaillen EU Blockchain Observatory and Forum, 2022, s. 16.

3.2.2 Lohkoketjuteknologian vaikutus tiedustelun suunnittelu-, keräys-, käsittely- ja jakeluvaiheisiin

Tiedustelutoiminnassa haasteita ovat muun muassa tiedon oikeellisuus, luottamuksellisuus ja saatavuus. Lohkoketjuteknologia tarjoaa näiden varmistamiseksi keinoja, joskin niiden kehittämistyö on edelleen kesken. Nykyiset teknologiat keskittyvät tiedon varastointiin ja jakamiseen salatuilla, mutta keskitetyillä varastointimenetelmillä, jotka ovat hyökkäyksille alttiita. Myös muita potentiaalisia lohkoketjun käyttötapoja on tutkittu tiedustelutoiminnassa (Razali, 2021). Kryptovaluuttojen (ja miksei muidenkin sovellusten) käyttäjät saattavat käyttää erilaisia palveluja transaktioiden häivyttämiseksi (Salisu ym., 2022). Muun muassa tämän takia lohkoketjuissa omistussuhteiden muutosten tunnistaminen ja prosessointi on työlästä ja erittäin haastavaa. Tunnistaminen vaatii paljon yksityiskohtaista osaamista ja oikeanlaisia työvälineitä ja aikaa, jolloin lopputuotteen toimittamiseen kuluva aika kasvaa. Toisaalta lohkoketjuteknologian levitessä erityisesti julkisen sektorin palveluihin ja ratkaisuihin, tiedon oikeellisuus ja luotettavuus lisääntyy erilaisissa rekistereissä. Tämän seurauksena lähteiden luotettavuus lisääntyy. Omistussuhteiden läpinäkyvyys ja laaja pääsy lohkoketjuihin on merkittävää tiedustelun näkökulmasta. Esimerkkinä Ukraina ja Diia-palvelu (Ministry and committee digital transformation Ukraine, 2022).

Edellinen huomioiden, on selvää, että analyytikkojen ja tiedon kerääjien lohkoketjuosaamista tulee vahvistaa tiedustelun laadun parantamiseksi. Myös erilaisiin uusiin työkaluihin tulee perehtyä ja hankkia tiedusteluorganisaatioiden käyttöön, jotta lohkoketjussa tapahtuneiden omistussuhteiden muutosten seuraaminen on mahdollista. Tässä suhteessa lohkoketjun vaikutus analyysiin on ilmeinen. Lisäksi lohkoketjuteknologia on nuori, hitaasti ja jatkuvasti kehittyvä. Uusia sovellutuksia ja tietoa syntyy jatkuvasti. Tietomassa on valtava, jolloin objektiivista ja relevanttia tietoa voi olla hankala tunnistaa, joka vaikuttaa myös analyytikkoon ja analyysiin.

Lohkoketjulla on vaikutusta myös tiedon jakamiseen ja luotettavuuteen tiedusteluorganisaatioiden välisessä kommunikoinnissa. Tim Olson (2018) kuvaa IBM:n blogissa,

kuinka lohkoketjuun pohjautuvaa ajatusta voitaisiin hyödyntää tiedusteluprosessissa. Lohkoketjuja voisi hyödyntää tiedusteluorganisaatioiden välisessä tiedon jakamisessa sekä tiedon luotettavuuden varmistamisessa, sillä muutosten ja lisäysten tulee olla lohkoketjua ylläpitävien osien hyväksymiä. Samalla jokaisella analyysiin osallistuvalla analyytikolla olisi jatkuvasti pääsy lohkoketjun kautta ajantasaisimpaan tietoon. Samaa ajatusta konkretisoi myös Muhammad ym. (2020), kuvaten turvallisen datan jakamisen järjestelmän. Myös NATO (2020) argumentoi samaa. Lohkoketjuja hyödyntämällä voitaisi varmistaa luotettava ja peukaloimaton kommunikaatio ja datan varastointi tiedusteluorganisaatioissa ja organisaatioiden välillä.

3.3 Kvanttiteknologia (Quantum Technology)

3.3.1 Kvanttiteknologian määritelmä ja soveltamisaloja

Kvanttiteknologioilla tarkoitetaan teknologioita, jotka perustuvat kvanttimekaniikan periaatteisiin kuten superpositio ja lomittuminen (engl. entaglement). (Till & Pritchard, 2016) Ne ovat teknologioita, jotka ovat syntyneet niin kutsutusta toisesta kvanttivallankumouksesta. Ensimmäisen kvanttivallankumouksen myötä arkipäiväistyneet teknologiat, kuten ydinvoima, puolijohteet, laserit ja magneettikuvaus, pohjautuvat klassisiin teorioihin (Krelina, 2021). Kvanttiteknologiat puolestaan hyödyntävät fysiikan ilmiöitä, joita ei pystytä selittämään näiden teorioiden avulla. (Till & Pritchard, 2016)

Kvanttiteknologioilla ei ole yhtä yhteisesti määritettyä taksonomiaa. Erityisesti sotilaallisia sovellusaloja tarkastelevissa julkaisuissa teknologiat jaetaan usein kolmeen ryhmään: kvantti-instrumentit ja sensorit (sisältäen myös sijaintiin, navigointiin ja aikaan liittyvät teknologiat), kvanttitiedonsiirtojen salaus, sekä kvanttilaskenta. (Krelina, 2021.) Teknologioiden eri kehitysvaiheiden ja soveltamisalojen tarkemman tarkastelun vuoksi käytämme tässä tutkielmassa viisiryhmäistä jaottelua:

1. Kvanttikellot (muun muassa atomikellot) mahdollistavat globaaleista navigointisysteemeistä (GPS) riippumattoman paikannuksen. (Battersby, 2020)
2. Kvanttiviestintä (salaus- ja tiedonsiirto) käsittää niin kutsutun klassisen informaation turvallisen siirtämisen ja kvantti-informaation siirtämisen. Tämä pitää sisällään kvanttiverkoston (engl. network) luomisen. (Krelina, 2021.) Mahdollisia sovelluskohteita uskotaan olevan lähes kaikilla yhteiskunnan keskeisillä osa-alueilla mukaan lukien terveydenhoito, puolustus ja kriittinen infrastruktuuri. (Till & Pritchard, 2016.)
3. Sensorit ja mittarit (engl. sensing and measurement) käsittäen muun muassa paine-, magneetti- ja kaasusensorit. Kvanttisensorit voivat paitsi parantaa sensoreiden tarkkuutta ja sensitiivisyyttä, myös mahdollistaa sellaisten suuruusluokkien tarkkailun, mikä perinteisillä sensoreilla ei ole mahdollista, kuten painovoiman, liikkeen ja sähkö- ja magneettikenttien tarkkailun. Ne myös lisäävä sensorien tehokkuutta ja tarkkuutta (Battersby S. 2020; Till & Pritchard, 2016; NATO, 2020)
4. Kvanttikuvantaminen (engl. imaging) paitsi parantaa nykyisten kuvausjärjestelmien tehoa, se voi myös mahdollistaa näkökentän ulkopuolella olevien asioiden ja painovoimakenttien näkyväksi tekemisen. Kuvaussysteemi mahdollistaa esimerkiksi nurkan taakse ja sumun läpi näkemisen. (Battersby 2020; Till & Pritchard, 2016)

5. Kvanttilaskenta (engl. computing) käyttää kvanttimekaniikkaa suurien tietomäärien käsittelemiseen nopeammin kuin perinteiset tietokoneet. Sen uskotaan muodostavan perustan tulevaisuuden supertietokoneille, joiden odotetaan ylittävän nykyisen teknologian esimerkiksi mallinnuksen, kryptografian ja tekoälyn aloilla. Ne mahdollistavat uusien materiaalien ja bioteknologian alan sovellusten kehittämisen. Kun kvanttitietokoneet tavoittavat tarvittavan kypsyystason (kvanttiylivalta), pystyy niiden laskentateho murtamaan nykyiset salausmenetelmät. (NATO, 2020)

Odotukset kvanttiteknologiaa kohtaan ovat suuret, ja sen uskotaan mullistavan muun muassa telekommunikaatiota ja tietoturvaa sekä puolustusteollisuutta. (Battersby, 2020; Krelina, 2021; Nato, 2020.) Kvanttiteknologian sovellukset näkyvät jo nyt eri aloilla (tosin hyvin rajallisesti), kuten ilmailuteollisuudessa, pankkisektorilla ja kemian teollisuudessa. Esimerkiksi turvallisia kvanttiviestintään pohjautuvia järjestelmiä käytetään jo maailmanlaajuisesti. Näistä esimerkeistä huolimatta kvanttiteknologiat ovat kuitenkin vielä pitkälle tutkimus- ja testausvaiheessa. Bettersbyn (2020) mukaan kvanttikelloissa ja kvanttiviestinnässä ollaan suhteellisen kypsällä tasolla, ja niiden kaupallisia sovelluksia on jo markkinoilla. Kvanttisensorien ja kuvantamisteknologioiden uskotaan saavuttavan niin kutsutun markkinakyvykkyyden seuraavan 5–10 vuoden aikana. Suurta läpimurtoa erityisesti kvanttilaskennan osalta odotetaan kuitenkin edelleen, sillä ”hypestä” huolimatta, kvanttitietokoneet ovat vielä lapsenkengissä, eikä niiden uskota saavuttavan markkinakelpoisuutta vielä seuraavaan 10–15 vuoteen. (Battersby, 2020; Acín ym. 2018)

3.3.2 Kvanttiteknologioiden vaikutus tiedustelun suunnittelu-, keräys-, käsittely- ja jakeluvaiheisiin

Kvanttiteknologioiden voidaan nähdä luovan uusia mahdollisuuksia myös tiedusteluyhteisölle. Tällä hetkellä suurin potentiaali liittynee kvanttisensoreihin, kuvantamiseen ja kvanttiviestintään, erityisesti tietoturvaan ja salausten purkuun, sekä kvanttikelloihin. Tulevaisuudessa kvanttilaskennan uskotaan lisäävän datan käsittelykykyä luoden uusia uhkia ja mahdollisuuksia kansalliselle turvallisuudelle ja tiedustelukyvyille. Pohdimme seuraavaksi kehitteillä olevan kvanttiteknologian soveltuvuutta tiedusteluprosessin eri vaiheisiin.

Kvanttitietokoneita voidaan mahdollisesti hyödyntää tulevaisuudessa tiedustelutehtävien suunnittelussa ja tarkennuksessa. Sovellusmahdollisuudet liittyvät kvanttilaskennan prosessointitehon hyödyntämiseen tekoälyavusteisten tiedustelukysymysten asettamisessa ja esimerkiksi tietokartoitusten tekemisessä. Vaikka koneiden kehittämistyö on vielä kesken, on mahdollista, että lähitulevaisuudessa kvanttialgoritmeja voidaan hyödyntää erilaisten ongelmien ratkaisussa. (NATO, 2020) On kuitenkin huomioitava, että samalla kun kvanttitietokoneet voivat mullistaa organisaatioiden kyvyn käsitellä tietoa, vaatii niiden käyttö myös erityisosaamista.

Sensoriteknologiat ovat toistaiseksi vielä testausvaiheessa, mutta läpimurtoa niiden hyödyntämiseksi odotetaan lähitulevaisuudessa. (NATO, 2020) Kvanttiteknologian myötä sensoreiden tarkkuus, tehokkuus ja kyvykkyys tarkkailla uusia määreitä/aineita, mukaan lukien painovoima, sähkö- ja magneettikentät, laajentaa signaalitiedustelun (erityisesti elektronisen mittaustiedustelun), geotiedustelun ja mittaus- ja tunnusmerkkitiedustelun datan keräystä. Kvanttitutkajärjestelmät mahdollistavat ilmassa ja avaruudessa erittäin pienitehoisen ja siten vaikeasti havaittavan tutkajärjestelmän käytön.

Painovoimasensorit mahdollistavat maan- ja vedenalaisen kuvantamisen, ja siten esimerkiksi vedenalaisten kohteiden kartoituksen. Kvanttikellot parantavat ajan mittaamisen tarkkuutta, vahvistavat navigointikykyä ja vähentävät riippuvuutta satelliittinavigointijärjestelmistä (engl. Global Navigation Satellite Systems, GNSS). Tämä puolestaan mahdollistaa datan keruun (navigoinnin) myös alueilla, jotka ovat satelliittinavigoinnin katvealueilla. Kvanttikuvantaminen mahdollistaa 3-ulotteisen (3D) ja jopa lähestyvien, näkökentän ulkopuolella olevien objektien kuvaamisen. Kuvantaminen mahdollistaa myös esteiden taakse näkemisen sekä esimerkiksi erilaisten kaasujen kuvaamisen. Nämä tarjoavat mahdollisuuksia erityisesti kuvaustiedustelun datan keruussa. Tehokkuutensa ja monipuolisuutensa ansiosta kvanttiteknologiat mahdollistavat valtavien datamassojen keräämisen kohteista, mihin perinteiset sensorit eivät kykene. (NATO, 2020)

Kvanttiviestinnän tärkein sovellusala liittynee tietoturvaan ja salausmenetelmien kehittämiseen. Tiedusteluyhteisön näkökulmasta vaikutus liittyy toisaalta datan keräämiseen ja kohteen salausten murtamiseen, toisaalta omien tietojen suojelemiseen salausmenetelmiä vahvistamalla. Vaikka kvanttilaskenta ei vielä toistaiseksi ole mahdollistanut monimutkaisten salausten purkamista, tulee tämä mahdollisuus huomioida jo nyt. Tilanne on erityisen kriittinen salaisen ja pitkään säilytettävän tiedon osalta, kuten esimerkiksi puolustusjärjestelmää tai ydinteknologiaa koskien. Vaikka nämä tiedot ovat tällä hetkellä tehokkaasti salattuja, eikä niiden purkaminen välttämättä onnistu supertietokoneilla, voidaan anastetut tiedot tallettaa odottamaan myöhempää salauksen murtamista. (IISS, 2019.)

Suurimmat mahdollisuudet tiedonkäsittelyvaiheen osalta liittyvät kvanttilaskentaan. Kvanttiteknologioiden hyödynnettävyys datan käsittelyvaiheessa on toistaiseksi vähäistä, mutta tulevaisuudessa mahdollisuuksia on runsaasti. Kvanttilaskenta voi jatkossa mahdollistaa salauksien purkamisen. Kerätty, varastoitu ja purkamaton tieto voidaan vuosien jälkeen purkaa ja ottaa analysoitavaksi. Salausten purkamisen ohella kvanttilaskennan uskotaan tuovan tehoa myös suurten datamassojen käsittelyyn. Useat tiedusteluprosessin toiminnot vaativat useiden datalähteiden ja monimutkaisen informaation käsittelyä sekä aikakriittisten analyysien tekemistä. Kvanttitietokoneen laskentateho yhdistettynä tekoälyavusteisiin teknologioihin ja koneoppimiseen voi lisätä tiedonkäsittelyn tehokkuutta ja tarkkuutta muun muassa hahmontunnistuksen (engl. pattern recognition) kautta. (NATO, 2020)

Kvanttiteknologioiden mahdollisuudet tiedusteluprosessin jakeluvaiheessa liittyvät erityisesti aineistojen turvalliseen jakamiseen. Erilaisten salausmekanismien kehittyminen voi tulevaisuudessa mahdollistaa isojen datamassojen jakelun kumppaneille turvallisesti. Kvanttiallekirjoitukset voivat myös lisätä salatun tiedon luotettavuuden todentamista. Ne toimivat nykyisten sähköisten allekirjoitusten tavoin ollen kuitenkin niitä huomattavasti tietoturvallisempia.

3.4 Esineiden internet (Internet of Things)

3.4.1 Määritelmä ja sovellutukset

Esineiden internetillä (engl. Internet of Things, IoT) tarkoitetaan järjestelmää, jossa toisiinsa yhteydessä olevat laitteet keräävät dataa ja kommunikoivat keskenään palveluiden tarjoamiseksi (Alhalafi & Veeraraghavan, 2019; Lee & Lee, 2015; Paolone ym., 2022). Asghari ym. (2019) luokittelevat esineiden internetin käyttötarkoitustensa perusteella terveydenhuollon, ympäristön, älykkäiden kaupunkien, liiketoiminnan ja teollisuuden

sovelluksiin. Esineiden internetin jakaminen luokkiin ainoastaan mahdollisten käyttötarkoitusten perusteella ei kuitenkaan välttämättä ole mielekästä, sillä esineiden internetin järjestelmät ovat jo nykyisellään hyvin moninaisia ja teknologian hyödynnettävyyden mahdollisuudet lisääntyvät ja kehittyvät jatkuvasti. Tässä raportissa esineiden internetiä tarkastellaan mahdollisten sovellusten lisäksi myös toiminnallisuuksien näkökulmasta, sillä niiden tarkastelu auttaa selvittämään teknologian hyödynnettävyyttä tiedustelun käyttötarkoituksiin myös tulevaisuudessa.

Alkhabbas ym. (2019) määrittelevät esineiden internetin laitteiden jakautuvan kolmeen tyyppiin: älykkäisiin esineisiin, antureihin ja/tai toimilaitteisiin sekä yhdyskäytäviin. Älykkäät esineet ovat ohjelmiston sisältäviä viestintään ja laskentaan kykeneviä esineitä, kuten älykelloja tai autoja. Suurin osa esineiden internetin laitteista on antureita ja/tai toimilaitteita, joissa on vain vähäinen laskentateho. Myös älykkäät esineet voivat sisältää sensoreja ja toimilaitteita. Yhdyskäytävät tukevat esineiden internetin toimintaa ja ovat liittymäkohtia järjestelmän eri esineiden välillä, mutta eivät itsenäisesti käsittele syötteitä. Esineiden toiminnallisuudet jaetaan aistimiseen (engl. sensing), liikuttamiseen (engl. actuating), aistimiseen ja liikuttamiseen (engl. sensing and actuating), säilyttämiseen (engl. storage) ja käsittelyyn (engl. processing). Merkittävää esineiden internetin esineiden toiminnallisuuksissa on vuorovaikutussuhde fyysiseen maailmaan. Esineiden internetin sovellukset voivat antureiden avulla aistia fyysisen maailman ilmiöitä, kuten lämpötilaa, painetta tai äänenvoimakkuutta ja olla toimilaitteiden kautta vuorovaikutuksessa ympäristöönsä. (Alkhabbas ym., 2019; Lee & Lee, 2015; Paolone ym., 2022).

Esineiden internetiä on kuvattu Internetin seuraavaksi kehitysaskeleeksi ja onkin arvioitu, että esineiden internetin laitteiden lukumäärä kolminkertaistuu 2020-luvun aikana, saavuttaen lähes 30 miljardin laitteen kokonaismäärän vuonna 2030 (Statista, 2022) Esineiden internetin kasvun mahdollistajana toimivat muun muassa nopean tiedonsiirron mahdollistavat 5G- ja 6G-teknologiat ja suuremman IP-osoiteavaruuden tarjoava IPv6, jonka myötä internetiin on mahdollista liittää huomattavasti aiempaa enemmän laitteita.

Erilaisten IoT-laitteiden ja teknologioiden nopea määrän kasvu markkinoilla on monelta osin tapahtunut turvallisuuden ja yksityisyyden kustannuksella. Esineiden internetin laitteiden varsinaisten käyttötarkoitusten lisäksi myös erilaiset haavoittuvuudet voivat tarjota uusia mahdollisuuksia myös tiedustelulle. Esimerkiksi Yhdysvaltain kansallinen turvallisuusvirasto NSA (National Security Agency) on varoittanut IoT-kalusteiden lisääntymisen tuottamista riskeistä toimistoympäristöissä (CSO, 2018). Esineiden internetin laitteet voivat sisältää takaportteja, jotka luovat esimerkiksi ulkomaiselle tiedustelupalvelulle mahdollisuuden vuorovaikutukseen laitteiden kanssa tai pääsyn laitteiden keräämään dataan. Erityisesti Kiina on merkittävässä asemassa esineiden internetin markkinoilla. (Alhalafi & Veeraraghavan, 2019; CSO, 2018; Paolone ym., 2022).

3.4.2 Esineiden internetin vaikutus tiedustelun suunnittelu-, keräys-, käsittely- ja jakeluvaiheisiin

Gilchrist (2017) toteaa esineiden internetin tarjoavan valtavasti uusia valvontamahdollisuuksia ihmisten jokaisen liikkeen, tekemisen ja toiminnan seurantaan ja vakoiluun. Todennäköisesti monet kuluttajamarkkinoillakin olevista laitteista tarjoavat oletusarvoisesti tiedustelun hyödynnettävissä olevaa dataa toimintaansa liittyvien sensoreiden kautta. Lienee myös mahdollista, että IoT-laitteita valmistavat yritykset asentavat laitteisiinsa kotimaansa tiedustelupalvelun ohjauksessa laitteen toiminnan kannalta

epäolennaisia sensoreita tai ominaisuuksia, joita voidaan tarvittaessa hyödyntää tiedustelutiedon keräämiseen. Esineiden internetin eksponentiaalisesti kasvava laitemäärä tarjoaa mahdollisuuksia suuren datamäärän keräämiseen. On huomionarvoista, että esineiden internetin tuottamaa dataa voidaan kerätä myös vieraan valtion alueella käyttämättä lainkaan omia laitteita, hyödyntämällä IoT-laitteille ja sovelluksille tyypillistä heikkoa tietoturvaa (Alhalafi & Veeraraghavan, 2019; Gilchrist, 2017). Näin tiedustelutoimintaa voidaan harjoittaa ulkomailla kyberympäristölle tyypillisen attribuutio-ongelman ja kiistettävyyden avulla; on hyvin vaikeaa osoittaa aukottomasti, kuka kyberympäristössä suoritetun toiminnan taustalla on. Esineiden internetin sovellukset luovat siis uusia mahdollisuuksia olla vuorovaikutuksessa fyysiseen ympäristöön kyberympäristön kautta. Erilaisten sensoreiden avulla tietoa voidaan kerätä lähes mistä tahansa fyysisestä ilmiöstä, joten on helppoa nähdä miten esineiden internetistä voi olla hyötyä esimerkiksi signaalitiedustelussa, mittaus- ja tunnusmerkkitiedustelussa ja geotiedustelussa. Esimerkiksi vuonna 2017 uutisoitiin Yhdysvaltain sotilaiden käyttämien urheilukellojen harjoitusdatan sijaintitietojen paljastavan sotilastukikohtien sijainteja. (Hern, 2018.) Esineiden internet tarjoaa mahdollisuuksia myös avointen lähteiden tiedusteluun. Esimerkiksi internetissä ilman suojausta olevien valvonta-, liikenne- ja kelikameroiden kuvaa voidaan käyttää tiedonhankintaan.

Esineiden internet voi tarjota myös uudenlaisia keinoja tiedon prosessointiin ja analysointiin. Laitteiden oman prosessointikapasiteetin ja pilvilaskennan lisäksi esineiden internetin yhteydessä puhutaan reunalaskennasta ja sumulaskennasta. Laitteiden tuottamaa suurta datamäärää ei ole välttämättä tarpeellista, saati kannattavaa siirtää pilveen, vaan laskentaa voidaan tehdä paikallisen verkon tasolla (sumulaskenta) tai laitteiden tasolla (reunalaskenta). Näin prosessointia voidaan tehdä myös ilman yhteyttä internetiin. Esineiden internetin tarjoama prosessointi- ja analysointikapasiteetti voi tarjota esimerkiksi mittaus- ja tunnusmerkkitiedustelulle uudenlaisia mahdollisuuksia, erityisesti jos datan analysointiin käytetään tekoälyä. Useista laitteista koostuva esineiden internetin ekosysteemi voisi kerätä dataa eri taajuusalueilla ja menetelmillä, sekä hyödyntää tekoälyalgoritmeja datan normalisoinnissa ja vertaamisessa referenssituntomerkkeihin. (Paolone ym., 2022).

Gilchristin (2017) mukaan olisi hölmöä ajatella, ettei esimerkiksi Australian, Kanadan, Uuden-Seelannin, Yhdistyneen Kuningaskunnan ja Yhdysvaltojen muodostama Five Eyes (FVEY) tiedusteluyhteistyön organisaatio selvittäisi esineiden internetin tarjoamia mahdollisuuksia tunnistamiseen, valvontaan ja sijaintitietojen keräämiseen. Esineiden internetin merkittävin hyöty tiedustelukäytössä tullaan todennäköisesti saavuttamaan yhdistämällä siihen muiden tässä raportissa esiteltyjen teknologioiden ominaisuuksia. Esimerkiksi tekoälyn käyttäminen esineiden internetin sensoreiden tuottaman datan analysointiin ja prosessointiin voi nopeuttaa ja helpottaa tiedusteluprosessia merkittävästi. Selvää on kuitenkin se, että esineiden internetin merkitys tiedustelukäytössä tulee kasvamaan internetiin liitettyjen laitteiden määrän jatkuvasti lisääntyessä.

4 Johtopäätökset

Jatkuvasti kehittyvät ja muuntuvat disruptiiviset teknologiat luovat tiedustelutoiminnalle uusia mahdollisuuksia, mutta myös täysin uudenlaisia uhkia. Teknologiat muun muassa automatisoivat tiedusteluun liittyvää manuaalista työtä ja päätöksentekoa, mahdollistavat suurten datamäärien keräämisen ja käsittelyn uusilla tavoilla sekä luovat

uusia keinoja tiedon luotettavuuden ja turvallisuuden varmistamiselle. Samalla teknologioiden kehittyminen tulee ottaa huomioon vastatiedustelussa ja varmistaa, että teknologioiden omalle toiminnalle aiheuttamat riskit on hallittu.

Koneoppiminen, lohkoketjut, kvanttiteknologia ja esineiden internet vaikuttavat erillisinä disruptiivisina teknologioina tiedustelun eri vaiheisiin ja metodeihin. Todellinen potentiaali saavutetaan kuitenkin teknologioiden vahvuuksia yhdistelemällä. Tiedustelun suunnitteluvaiheessa voidaan esimerkiksi hyödyntää kvanttilaskennan prosessointitehon nopeuttaman tekoälyn käsittelemää tietoa tiedustelutoimeksiannon ja -kysymyksen jalostamiseen. Tiedustelun keräysvaiheessa voidaan käyttää laajaa esineiden internetiin kytkettyä ja edistynyttä kvanttiteknologiaa ja -kuvantamista hyödyntävää sensoriverkkoa tai lohkoketjua valtavien datamäärien keräämiseen. Keräysvaiheessa tekoäly voi myös rajata datasta epäoleellista kohinaa ja siten esimerkiksi pienentää datan säilyttämisen ja siirtämisen resurssien kuormitusta.

Suurten datamäärien hyödyntäminen vaatii jatkuvasti kehittyneempää tiedustelutiedon käsittelyä. Tekoäly voi nopeastikin löytää suuresta määrästä dataa sellaisia yhteyksiä, joita ihmisen ei ylipäätään olisi mahdollista havaita. Kvanttilaskennan kehittyessä myös tiedon käsittelynopeus kasvaa jatkuvasti. Esineiden internet mahdollistaa tiedon käsittelyn laitteiden tai paikallisen verkon tasolla. Tekoälyn vahvistamana ennalta määritettyjen herätteiden nostaminen tiedusteluorganisaation käyttöön on mahdollista.

Jakeluvaiheessa lohkoketjulle ominainen tiedon luotettavuus ja muuttumattomuus ja läpinäkyvät omistussuhteet tarjoavat uudenlaisia mahdollisuuksia tiedustelun kansainväliselle yhteistyölle ja tekoälyavusteiseen tiedon jakamiseen asiakkaalle automaattisesti ja reaaliaikaisesti. Kvanttiallekirjoitukset helpottavat tiedon luotettavuuden todentamista ja aiempaa tehokkaammat salaukset mahdollistavat suurten tietomäärien jakamisen turvallisesti.

Tiedusteluun liittyvien teknologioiden kehittyminen voi aiheuttaa riskejä tiedustelupalveluiden toiminnalle sekä kansalaisten yksityisyydelle. Jos vieraan valtion organisaatio onnistuu hyödyntämään uusia teknologioita vakoilutarkoituksessa, voi oman tiedusteluorganisaation operatiivinen turvallisuus vaarantua. Esimerkiksi kvanttiteknologiaa voidaan hyödyntää aiemmin vahvoina pidettyjen salausten purkamisessa ja esineiden internetin heikkoa tietoturvaa laitteiden vakoilussa. Muun muassa tästä syystä näiden disruptiivisten teknologioiden hyödyntäminen on merkittävä kohde myös vastatiedustelulle. Kehittyvän teknologian myötä loukkaukset yksilöiden perusoikeuksiin ja vapauksiin, kuten yksityisyyteen, voivat myös olla ennalta arvaamattomia. Mahdolliset negatiiviset vaikutukset voivat ilmetä ulkomaisen ja kotimaisen tiedustelutoiminnan seurauksena. Negatiivisten seurausten vähentämiseksi olisikin tärkeää, että lainsäädäntö pystyisi seuraamaan teknologian nopeaa kehitystä ja vastatiedustelu kykenisi vahvistamaan puolustusta kansalaisiin kohdistuvaa vakoilua vastaan.

Raportissa esitellyt teknologiat ovat kehityskaarillaan eri vaiheissa. Siinä missä tekoälylle, esineiden internetille ja lohkoketjulle löytyy jo erilaisia kaupallisia sovelluksia, on kvanttiteknologia vielä lapsenkengissä. Toisaalta mikään teknologioista ei vielä ole saavuttanut lopullista potentiaaliaan, vaan kehittyy edelleen. Selvää on, että näiden teknologioiden kehityksen seuraaminen on erilaisten tiedusteluorganisaatioiden näkökulmasta hyvinkin kiinnostavaa ja niiden tarkoituksenmukainen soveltaminen voi mullistaa tiedustelun kenttää ennennäkemättömällä tavalla. On mahdollista, ja jopa todennäköistä, että uusiin teknologioihin liittyvä kilpavarustelu on jo hyvässä vauhdissa ja tiedustelupalveluiden käytössä oleva teknologia on jo yleisesti tunnettua edistyneempää.

Tiedusteluorganisaatioiden kyvykkyyksistä ei viestitä avoimesti ja erityisesti valtioiden rahoittamilla organisaatioilla voi olla resursseja parhaan mahdollisen osaamisen ja kehittyneimmän teknologian hankkimiseen.

Disruptiivisten teknologioiden vaikutukset tiedustelutoiminnalle näkyvät jatkuvasti kasvavana datamääränä, mutta toisaalta myös datan käsittelyn kehittymisenä. Tämän kehityskulun myötä myös mahdollisuudet luotettavan ja käyttökelpoisen tiedustelutiedon jalostamiselle kasvavat. Tiedustelulla on pitkä historia uusien teknologioiden hyödyntämisessä, ja mullistukset luovat mahdollisuuden etulyöntiaseman saavuttamiselle. Vaikka kehittyvät teknologiat eivät olekaan syrjäyttäneet ihmistä tiedusteluprosessissa, tulee niiden rooli ja niiden hyödyntämisen osaamistarpeet kasvamaan tiedusteluorganisaatioissa.

Joskus on vaarallista saada sitä, mitä haluaa. Vaikka tiedustelutoimien on aina palveltava asiakkaan tietopyyntöä, on kysymys ammattietiikan kannalta monimutkaisempi. Tiedustelutiedon tuottajan tulee jakaa asiakkaalle kokonaiskuva, joka voi olla selkeä tai myös kompleksinen. Myös päätöksentekijän on hyvä altistua tiedustelutiedolle, jonka sisältöä hänen täytyy pureksia ja jonka muoto heijastaa käsitellyn tiedon kompleksisuutta. Tästä näkökulmasta on syytää pohtia, miten tarkoituksenmukaista on antaa päätöksentekijälle valta määrittää muoto, jossa tekoäly tiedustelutuotteen jakaa. Kysymys kuuluukin, kuinka pitkälle olemme valmiita päästämään koneen tekemään tiedustelutoiminnan eri vaiheita?

Lähteet

Acín, A., Bloch, I., Buhrman, H., Calarco, T., Eichler, C., Eiser, J., Esteve, D., Gisin, N., Glaser, S., Jelezko, F., Kuhr, S., Lewenstein, M., Riedel, M., Schmidt, P.O., Thew, R., Wallraff, A., Walmsley, I., Wilhelm, F.K. (2018). The quantum technologies roadmap: a European community view. New Journal of Physics, (20) 080201.

Alhalafi, N., & Veeraraghavan, P. (2019). Privacy and Security Challenges and Solutions in IOT: A review. IOP Conference Series: Earth and Environmental Science, 322(1), 012013. https://doi.org/10.1088/1755- 1315/322/1/012013

Alkhabbas, F., Spalazzese, R., & Davidsson, P. (2019). Characterizing Internet of Things Systems through Taxonomies: A Systematic Mapping Study. Internet of Things, 7, 100084. https://doi.org/10.1016/j.iot.2019.100084

Akter, R., Golam, M., Lee, J. M., & Kim, D. S. (2021). Blockchain Assisted Unauthorized Target Localization for C4I Communication Network Using Convolution Neural Network. Proceedings of the Korea Telecommunications Society Conference, 407-408.

Asghari, P., Rahmani, A. M., & Javadi, H. H. S. (2019). Internet of Things applications: A systematic review. Computer Networks, 148, 241–261. https://doi.org/10.1016/j.comnet.2018.12.008

Bank of Jamaica. (31.12.2021). BOJ's CBDC Pilot Project a Success. https://boj.org.jm/bojs-cbdc-pilot-project-a-success/

Bank of Russia. (13.10.2020). The digitalisation of the economy and the development of financial technologies generate public demand for new, advanced payment methods. https://www.cbr.ru/eng/analytics/d_ok/dig_ruble/

Battersby, S. (toim.) (2020). The Quantum Age: technological opportunities. Government Office for Science. BBC (2.6.2018). Are you scared yet? Meet Norman, the psychopathic AI. https://www.bbc.com/news/technology-44040008.

Boucher, P. N. (2020). Artificial intelligence: How does it work, why does it matter, and what can we do about it? European Parliament, 2020, https://data.europa.eu/doi/10.2861

Bower, J. L. & Christensen, C. M. (1995). Disruptive technologies: catching the wave. Harward Business Review.

Christensen, C. M. & Raynor, M. E. (2003) The Innovator's Solution: Creating and Sustaining Successful Growth. Boston. Harvard Business School Press. CSO. (31.10.2018). Beware the IoT spy in your office or home via smart furniture, warns NSA. CSO (Online). https://www.proquest.com/docview/2127489143/abstract/5DF59D98C A7B4FB7PQ/1.

Department of homeland security. (9.7.2019). Snapshot: S&T's Blockchain program focuses on security, privacy, interoperability & standards. Haettu 7. marraskuuta 2022 osoitteesta https://www.dhs.gov/science-andtechnology/news/2019/07/09/snapshot-blockchain-and-dhs.

Diia. (2022). Online public services. Haettu 4. marraskuuta 2022 osoitteessa https://diia.gov.ua/.

EU Blockchain Observatory and Forum (2022). EU blockchain Ecosystem developments. Haettu 8. marraskuuta 2022 osoitteessa https://www.eublockchainforum.eu/sites/default/files/reports/eu_ecos ystem_report_20220909_final%20version_1.pdf.

Euroopan parlamentti ja neuvosto. Asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).

Foroglou, G., & Tsilidou, A. L. (2015). Further applications of the blockchain. In 12th student conference on managerial science and technology (9).

Gilchrist, A. (2017). IoT security issues (1. painos). DE-G Press.

Gobble, M., (2016) Defining Disruptive Innovation. Research. Technology Management, 59(4), pp. 66-71.

Haque, A. B., Islam, A. N., Hyrynsalmi, S., Naqvi, B., & Smolander, K. (2021). GDPR compliant blockchains–a systematic literature review. IEEE Access (9), 50593-50606. Hern, A. (28.4.2018). Fitness tracking app Strava gives away location of secret US army bases. The Guardian. https://www.theguardian.com/world/2018/jan/28/fitness-trackingapp-gives-away-location-of-secret-us-army-bases.

Hsiao, JH., Tso, R., Chen, CM., Wu, ME. (2018). Decentralized E-Voting Systems Based on the Blockchain Technology. Teoksessa Park, J., Loia, V., Yi, G., Sung, Y. (toim.) Advances in Computer Science and Ubiquitous Computing. Lecture Notes in Electrical Engineering, Vol 474. Springer, Singapore.

Hershkovitz, S. (2022). The Future of National Intelligence: How Emerging Technologies Reshape Intelligence Communities. Rowman & Littlefield Publishers.

Hulnick, A. S. (2006). What's wrong with the Intelligence Cycle. Intelligence and national Security, 21(6), 959-979. IBM. (3.6.2020). IBM Artificial intelligence (AI). https://www.ibm.com/cloud/learn/what-is-artificial-intelligence.

IISS. (2019). The Military Balance 2019. International Institution for Strategic Studies. https://www.iiss.org/publications/the-military-balance/themilitary-balance-2019.

Katz, B. (2020). The intelligence edge: Opportunities and challenges from emerging technologies for U.S. intelligence. Center for Strategic & International Studies. https://www.csis.org/analysis/intelligence-edge-opportunitiesand-challenges-emerging-technologies-us-intelligence.

Krelina M. (2021). Quantum technology for military applications, EPJ Quantum Technology, 8(24). https://doi.org/10.1140/epjqt/s40507-021-00113-y.

Lansiti M, Lakhani K,R. (2017). The truth about Blockchain. Harvard Business Review, 95(1), 119–127.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431–440. https://doi.org/10.1016/j.bushor.2015.03.008

Lowenthal, M & Clark, R. (2016). The 5 Disciplines of Intelligence Collection. SAGE. McDowell, D. (2009). Strategic Intelligence: A Handbook for Practitioners, Managers, and Users. Scarecrow Press.

Merriam-Webster. (ei pvm). Blockchain. Haettu 31. lokakuuta 2022 osoitteesta https://www.merriam-webster.com/dictionary/blockchain.

Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here, julkaisussa IEEE 18th International Conference on e-Health Networking, Applications and Services, 1-3. doi: 10.1109/HealthCom.2016.7749510.

Ministry and committee digital transformation Ukraine. (2022). Diia - online public services. Haettu 8. marraskuuta 2022 osoitteesta http://diia.gov.ua.

Muhamad, W. N. W., Razali, N. A. M., Wook, M., Ishak, K. K., Zainudin, N. M., Hasbullah, N. A., & Ramli, S. (2020). Evaluation of Blockchain-based Data Sharing Acceptance among Intelligence Community. International Journal of Advanced Computer Science and Applications, 11(12).

Muller, E. (2020). Delimiting disruption: Why Uber is disruptive, but Airbnb is not. International Journal of Research in Marketing, 37(1), pp. 43-55. https://doi.org/10.1016/j.ijresmar.2019.10.004.

Nakamoto, S. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. Haettu 8. marraskuuta 2022 osoitteesta https://bitcoin.org/bitcoin.pdf

National Intelligence Council. (huhtikuu 2008). Disruptive Civil Technologies Six Technologies with Potential Impacts on US Interests out to 2025. Conference report.

NATO. (17.10.2022). Emerging and disruptive technologies. https://www.nato.int/cps/en/natohq/topics_184303.htm NATO. (2020).

NATO Science & Technology Organization. Science & Technology Trends: 2020–2040. NATO Science & Technology Organization. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/19042 2-ST_Tech_Trends_Report_2020-2040.pdf.

ODNI (2019). Strategic plan to advance cloud computing in the intelligence community. Office of national intelligence US. https://www.dni.gov/files/documents/CIO/Cloud_Computing_Strateg y.pdf.

OECD (2020). OECD Digital Economy Outlook 2020. OECD Publishing, Pariisi.

Olsson, T. (6.3.2018). IBM supply chain and blockchain blog. https://www.ibm.com/blogs/blockchain/2018/03/blockchain-for-intelligence-supply-chains/.

Paolone, G., Iachetti, D., Paesani, R., Pilotti, F., Marinelli, M., & Felice, P. D. (2022). A Holistic Overview of the Internet of Things Ecosystem. IoT, 3(4), 398–434. https://doi.org/10.3390/iot3040022

Peoples bank of China. (2022). Solidly carry out pilot research and development of digital RMB. Haettu 6. marraskuuta 2022 osoitteesta https://mp.weixin.qq.com/s/mrc_vPXAZf4glX9_NEfmUQ.

Putin, V. (2022) A Post-Hegemonic World: Justice and Security for Everyone, (puhe 27.10.2022 at valdai club). Haettu 8. marraskuuta 2022 osoitteesta http://en.kremlin.ru/events/president/transcripts/69695.

Razali, N. A. M., Wan Muhamad, W. N., Ishak, K. K., Saad, N. J. A. M., Wook, M., & Ramli, S. (2021). Secure Blockchain-Based Data-Sharing Model and Adoption among Intelligence Communities. IAENG International Journal of Computer Science, 48(1).

Salisu, S., Filipov, V., Penne, B. (2022). Blockchain forensics: A Modern approach to investigating Cyber Crime in the age of decentralization. Bilic.io

Shagina, M. (2022). Central Bank Digital Currencies and the implications for the global financial infrastructure: The transformational potential of Russia's digital rouble and China's digital renminbi, Fiia briefing paper, (329).

SAS (2021). Machine learning. Haettu 8. marraskuuta 2022 osoitteesta https://www.sas.com/en_in/insights/analytics/machine-learning.html.

Singh, A., Triulzi, G., Magee, C. L. (2021). Technological improvement rate predictions for all technologies: Use of patent data and an extended domain description, Research Policy, 50(9). https://doi.org/10.1016/j.respol.2021.104294.

Statista. (ei pvm.). IoT connected devices worldwide 2019-2030. Statista. Haettu 31. lokakuuta 2022 osoitteesta https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide

Stenfors, S. (2019). Lohkoketjut hypen jälkeen: Mitä kuuluu lohkoketjuja muihin hajautettuihin teknologioihin julkishallinnon näkökulmasta? Teoksessa Rousku K. (toim.), Andersson C., Stenfors S., Lähteenmäki I., Limnell J., Mäkinen K., Kopponen A., Kuivalainen M. ja Rissanen O-P., 2019, Pilkahduksia tulevaisuuteen: Tietopolitiikka, tekoäly ja robotisaatio hyvinvoinnin ja taloudellisen menestyksen mahdollistajana Suomessa, (Valtiovarainministeriön julkaisuja 2019:22), 69-78.

Suitto J, 2019, Kryptovaluuttojen käyttö rikollisessa toiminnassa [opinnäytetyö, Poliisiammattikorkeakoulu]. Thesus julkaisuarkisto https://www.theseus.fi/bitstream/handle/10024/265329/ON_Suittio.pd f

Thangavelu, P. (5.6.2020). Companies that failed to innovate and went bankrupt. https://www.investopedia.com/articles/investing/072115/companies-went-bankrupt-innovation-lag.asp.

Till S. & Pritchard J. (toim.) (2016). UK Quantum Technology Landscape 2016. UK Official DSTL/PUB098369. https://docslib.org/doc/11895633/uk-quantum-technology-landscape-2016#pf5d.

Utterback, J. & Acee, H. J. (2005). Disruptive technologies: An expanded view. International Journal of Innovation Management, 9(1), 1-17. Vergun, D. (8.3.2022). DOD in Search of Disruptive Technologies That Will Enable the Warfighter. https://www.defense.gov/News/News-Stories/Article/Article/2959378/dod-in-search-of-disruptive-technologies-that-will-enable-the-warfighter/

Xu, M., Chen, X. & Kou, G. (2019). A systematic review of blockchain. Financial Innovations, 5(27)

VENÄJÄN VALTIOLLISTEN TIEDUSTELUPALVELUIDEN KYBERTOIMINTA

Eero Heikkinen, Olli Hönö, Juho Saarinen

1 Johdanto

Erilaisilla kyberoperaatioilla vaikuttaminen on tänä päivänä keskeinen vaikuttamisen keino valtioiden kansainvälisissä suhteissa. Kyberoperaatioihin liittyy aina attribuutio-ongelma eli operaation toteuttaneen tahon osoittaminen varmuudella on vaikeaa. Vaikka menetelmät hyökkääjien tunnistamiseen kehittyvät koko ajan, niin myös hyökkääjien keinot ja tekniikat jälkien piilottamiseen tai niiden osoittamiseen muualle kehittyvät.

Yhdysvaltalainen ajatushautomo The Council on Foreign Relations ylläpitää tietokantaa, johon kerätään tietoja kyberoperaatioista, joiden taustalla on pystytty osoittamaan olevan valtiollinen toimija. Sen mukaan vuosina 2005–2021 Venäjä on pystytty osoittamaan 140 kyberoperaation tekijäksi. (The Council on Foreign Relations, 2022)

Viime vuosina länsimaiden viranomaiset ovat aiempaa suoremmin alkaneet nimeämään Venäjän usean hyökkäyksen tekijätahoksi. Yhdysvaltojen ja sen liittolaisten kyberturvallisuusviranomaiset julkaisivatkin yhteisen varoituksen Venäjän aiheuttamasta kyberuhasta kriittistä infrastruktuuria kohtaan. Varoituksen mukaan Venäjällä on merkittävä kyky kyberoperaatioihin ja historiaa sen käyttämisestä hyökkäyksellisiin toimiin. (U.S. Department of Defense, 2022)

Venäjän virallisista dokumenteista luettavissa olevassa doktriinissa Venäjä nimeää tavoitteiksi lähinnä puolustuksellisia puolia eikä ainuttakaan hyökkäyksellistä aspektia. (Lilly & Cheravitch, 2020) Venäjän doktriinissa painotetaan kuitenkin informaatioympäristön tärkeyttä. Maa nimesi sen omaksi operaatioympäristöksi jo kuusi vuotta ennen NATOa. Venäjällä ymmärretään informaatioympäristö eri tavalla kuin lännessä, Venäjä ei näe kyber- tai informaatioympäristöä ainoastaan informaatioteknologisena kokonaisuutena kuten lännessä, vaan myös informaatio-psykologisena. ”Informaatiosodankäynnin” ymmärretään sisältävän tietoverkko-operaatioita, elektronista sodankäyntiä, psykologisia operaatioita sekä informaatio-operaatioita. (Bagge, 2019)

Tämän raportin tarkoituksena on vastata seuraaviin kysymyksiin:

- Mitkä Venäjän turvallisuus- ja tiedustelupalvelut suorittavat kyberoperaatioita?
- Minkälaisia kyberoperaatioita ne ovat suorittaneet?
- Minkälaisia tavoitteita kyberoperaatioilla on?

Raporttia varten läpikäyty aineisto on julkista ja pääosin länsimaista alkuperää. Tästä johtuen raportin näkökulma on vahvasti läntinen. Raportissa käytetyt lähteet on pyritty arvioimaan kriittisesti. Työryhmällä ei ollut mahdollisuutta tutustua suoraan venäläiseen materiaaliin puutteellisen kielitaidon takia.

Raportin luvussa 2 käydään läpi Venäjän valtion turvallisuus- ja tiedustelupalveluita, jotka osallistuvat kyberoperaatioiden toteuttamiseen. Luvussa 3 käsitellään tunnettuja operaatioita, jotka on pystytty osoittamaan venäläisten toimijoiden tekemiksi. Luvussa 4 arvioidaan operaatioiden mahdollisia tavoitteita. Viimeisessä luvussa esitellään työryhmän raportin aineiston pohjalta tekemät johtopäätökset.

Raportti antaa lukijalle käsityksen siitä mitkä venäläisistä turvallisuus- ja tiedustelupalveluista toteuttavat kyberoperaatioita, minkä tyyppisiä operaatioita on toteutettu, mitkä ovat niiden tavoitteet sekä miten operaatioihin on reagoitu eri tahojen toimesta.

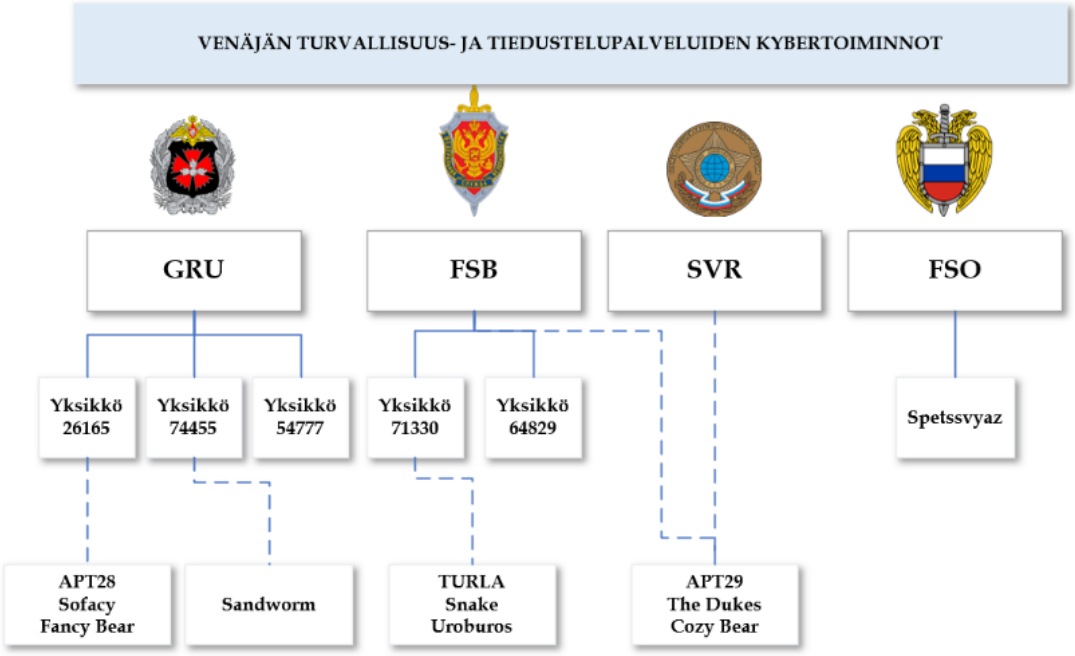
2 Turvallisuus- ja tiedustelupalvelut

Venäjän kyberoperaatiot ovat nykyisin hajautettu usean eri viraston kesken, eikä mikään yksittäinen turvallisuus- tai tiedustelupalvelu ole yksin vastuussa kyberoperaatioista. Nykyisen kaltainen organisointi sai alkunsa vuonna 2003 Presidentti Vladimir Putinin määräämän turvallisuuspalveluiden uudelleenorganisoinnin myötä. Sen johdosta valtion viestintä- ja informaatioviraston (FAPSI) toimintoja jaettiin uudelleen valtion sisäisen turvallisuuspalvelu FSB:n, ulkomaantiedustelupalvelu SVR:n sekä valtion suojauspalvelu FSO:n kesken. Edellä mainittujen turvallisuus- ja tiedustelupalveluiden lisäksi Venäjän asevoimien sotilastiedustelulla (GRU) on merkittävää kyberoperaatiokyvykkyyttä. (The Center for European Policy Analysis, 2022)

Uudelleenjärjestelyjen myötä panostus kyberoperaatioihin kasvoi, ja kuluneen 20 vuoden aikana Venäjä on lisännyt merkittävästi kyberoperaatioihin liittyvää henkilöstöään ja resurssejaan. Muutoksen myötä maa on onnistunut parantamaan kykyään entistä monipuolisempiin kyberoperaatioihin. (Congressional Research Service, 2022)

Kybertoimintojen hajaantuminen eri turvallisuuspalveluiden välille lisää kuitenkin niiden välistä kilpailua resursseista, henkilöstöstä ja vaikutusvallasta. Tämä on yhtenä mahdollisena syynä siihen, että venäläiset kyberyksiköt suorittavat joskus samantyyppisiä operaatioita ilman ilmeistä tietoa toisten yksiköiden operaatioista. (Congressional Research Service, 2022)

Kuviossa 1 on esitelty Venäjän turvallisuus- ja tiedustelupalveluiden sekä niihin liitettyjen kyberoperaatioita suorittavien ryhmien suhteita.



KUVIO 1 Venäjän turvallisuus- ja tiedustelupalveluiden kyberyksiköt (The Warsaw Institute, 2020)

2.1 FSB

Venäjän federaation turvallisuuspalvelu (FSB) vastaa maan sisäisestä turvallisuudesta ja vastatiedustelusta. Kybertoiminnoissa sen tehtäviin kuuluu Venäjän suojeleminen ulkomaisilta kyberoperaatioilta ja kotimaisten rikollisten hakkereiden tarkkailu. Viime vuosina FSB on laajentanut tehtäväänsä ulkomaisten tiedustelutietojen keräämiseen ja hyökkääviin kyberoperaatioihin. (Congressional Research Service, 2022) Kyberanalyytikot ovat arvioineet, että FSB:hen liitoksissa olevia hakkeriryhmiä ovat ainakin Berserk Bear, Energetic Bear, Gamaredon, Dragonfly ja Crouching Yeti (The Foreign, Commonwealth & Development Office, 2022).

FSB:n sisällä kybertoiminnot on jaettu kahteen erikoisyksikköön, jotka valvovat sen tietoturvaa ja kybertoimintoja. **Yksikön 71330** pääasiallinen tehtävä on elektronisen viestinnän kaappaaminen ja purkaminen sekä vieraiden valtioiden tai yritysten tietojärjestelmiin tunkeutuminen. Iso-Britannian ulkoministeriön raportin mukaan yksikkö 71330 on suorittanut kyberoperaatioita ainakin vuodesta 2010 alkaen. (The Foreign, Commonwealth & Development Office, 2022). **Yksikön 64829** päätehtävänä on kotimaahan kohdistuva kybertoiminta ja -turvallisuus. Sen tiedetään kuitenkin toteuttaneen myös joitakin ulkomaihin kohdistuneita kyberoperaatioita. (Congressional Research Service, 2022)

Yhdysvaltojen kongressin tutkimuspalvelun mukaan FSB:n yksiköt pystyvät valmistamaan omia kehittyneitä haittaohjelmia. Lisäksi FSB muokkaa verkosta saatavia haittaohjelmia matkiakseen muita hakkeriryhmiä tavoitteenaan salata FSB:n omaa toimintaa. Raportin mukaan FSB myös ohjaa koulutus- ja tutkimuslaitoksia, jotka tukevat suoraan FSB:n kyberoperaatioita. (Congressional Research Service, 2022)

Yhdysvaltojen hallituksen kyberturvallisuus ja infrastruktuurivirasto CISA (Cybersecurity & Infrastructure Security Agency) on varoittanut Venäjän tiedusteluviranomaisten ja erityisesti FSB:n yksikkö 64829:n toimista rekrytoida rikollisia hakkereita

toimintaansa mukaan (The Cybersecurity and Infrastructure Security Agency, 2022). FSB:n arvioidaankin käyttävän paljon myös rikollisia hakkereita laajentaakseen suorituskykyään sekä piilottaakseen omaa toimintaansa. Yhdysvaltojen oikeusministeriö onkin nostanut syytteitä useita venäläisiä hakkereita vastaan erilaisista rikollisista ja valtion tukemista kybertoimista. Monet näistä syytteistä valottavat rikollisten hakkereiden ja FSB:n välistä läheistä ja pitkäaikaista suhdetta. (The Department of Justice, 2017)

2.2 GRU

Venäjän federaation asevoimien sotilastiedustelu (GRU) on Venäjän pahamaineisimpien ja haitallisimpien kyberoperaatioiden takana. GRU ohjaa myös useita tutkimuslaitoksia, jotka auttavat kehittämään hakkerointityökaluja ja haittaohjelmia kyberoperaatioita varten. GRU:n kyberyksiköt tunnetaan halusta suorittaa röyhkeitä ja aggressiivisia operaatioita, joissa operaatioturvallisuus ja salassapito ovat usein pienemmässä roolissa. (Congressional Research Service, 2022) GRU:n kuudennen direktoraatin alaisuudessa toimii kolme erikoisyksikköä kyberoperaatioita varten, joilla jokaisella on omat vastuualueensa.

Yksikkö 26165 tunnetaan myös nimellä 85th Main Special Service Center. Yksikön uskotaan olevan APT28 (tunnetaan myös nimellä Fancy Bear) hakkeriryhmän taustalla. Länsimaiden tiedusteluviranomaiset ovat yhdistäneet yksikön kyberoperaatioihin lukuisia poliittisia, valtiollisia ja yksityisen sektorin kohteita vastaan Yhdysvalloissa ja Euroopassa. (Congressional Research Service, 2022) Yksikkö on yksi kahdesta venäläisestä ryhmästä, jotka Yhdysvaltain hallitus on nimennyt olevan vastuussa Hillary Clintonin vuoden 2016 presidentinvaalikampanjan hakkeroinnista (The Department of Justice, 2018).

Yksikkö 74455 tunnetaan myös nimellä Main Center for Special Technologies. Yksikkö on yhdistetty joihinkin Venäjän röyhkeimmistä ja vahingollisimmista kyberhyökkäyksistä ja sen uskotaan olevan Sandworm -hakkeriryhmän taustalla (U.S. Department of State, 2022). Yksikkö ei kuitenkaan pyri pelkästään tunkeutumaan tietojärjestelmiin ja keräämään tietoa. Sillä arvioidaan olevan merkittäviä hyökkäyksellisiä kybervalmiuksia, joiden avulla se pyrkii toteuttamaan muun muassa vieraan valtion keskeiseen infrastruktuuriin kohdistuvia kyberhyökkäyksiä. (Congressional Research Service, 2022)

Lokakuussa 2020 Yhdysvaltojen oikeusministeriö syytti yksikön jäseniä lukuisista kyberhyökkäyksistä, mukaan lukien NotPetya -haittaohjelmahyökkäyksestä vuonna 2017, Ukrainan hallitukseen ja infrastruktuuriin kohdistuneista hyökkäyksistä vuonna 2016 sekä vaikuttamisyrityksistä Ranskan 2017 presidentinvaaleihin. (The Department of Justice, 2020)

Yksikkö 54777 tunnetaan myös nimellä 72nd Special Service Center. Yksikkö on vastuussa GRU:n psykologisista operaatioista. Yksikön vastuulle kuuluvat myös verkossa tapahtuvat informaatiovaikuttamisen operaatiot. Yksikön tehtäviin kuuluu tukea muita GRU:n kyberyksiköitä sekä operointi taktisella tasolla suorittamalla elektronisen sodankäynnin operaatioita. Yhdysvaltojen kongressin tutkimuskeskuksen mukaan yksikkö on liitetty viime vuosina mm. disinformaatiokampanjoihin koronapandemiaan liittyen. (Congressional Research Service, 2021)

2.3 SVR

Venäjän federaation ulkomaan tiedustelupalvelu (SVR) vastaa ulkomaisen tiedustelutiedon keräämisestä henkilötiedustelun, signaalitiedustelun sekä eri kybertoiminnan

menetelmillä. SVR painottaa tiedon keräämistä, salassapitoa ja operaatioturvallisuutta eli se pyrkii toimimaan salassa. SVR:llä tiedetään myös olevan korkeatasoinen tekninen osaaminen, ja se pyrkii usein saamaan ja säilyttämään pääsyn kohteen tietojärjestelmiin pitkiä aikoja. (Congressional Research Service, 2022) Iso-Britannian kyberturvallisuusviranomaiset ovat viitanneet SVR:n hakkereihin myös nimillä APT 29, Cozy Bear ja Dukes (The National Cyber Security Center, 2021).

Yhdysvaltain hallitus nimesi SVR:ään liitetyn ryhmän APT29:n toiseksi kahdesta venäläisestä ryhmästä, jotka olivat vastuussa poliittisiin kampanjoihin murtautumisesta Yhdysvaltain 2016 presidentinvaalien aikana (The Cybersecurity and Infrastructure Security Agency, 2016). Viime vuosina SVR on liitetty lukuisiin kybervakoiluoperaatioihin. Huhtikuussa 2021 Yhdysvaltain hallitus totesi APT29:n olevan vastuussa SolarWinds-hyökkäyksestä, joka hyödynsi toimitusketjun haavoittuvuuksia soluttautuakseen Yhdysvaltain hallituksen ja yksityisen sektorin tietoliikenneverkkoihin. (The Cybersecurity and Infrastructure Security Agency, 2021)

2.4 FSO

Venäjän federaation suojauspalvelu (FSO) on vastuussa Venäjän hallituksen ja valtion henkilöstön fyysisestä sekä elektronisesta turvallisuudesta. Elektronisen turvallisuuden osalta tehtävää hoitaa FSO:n viestintä ja informaatiopalvelun erikoisyksikkö Spetssvyaz. Yksikön vastuulla on vieraiden valtioiden viestinnän keräys signaalitiedustelun keinoin, viestinnän purkaminen sekä Venäjän valtion viestintä- ja informaatiojärjestelmien suojaus. FSO:n tehtävä kyberoperaatioissa näyttää olevan ensisijaisesti puolustuksellinen eikä ole viitteitä siitä, että se olisi suorittanut hyökkäyksellisiä kyberoperaatioita. (Congressional Research Service, 2021)

3 Tunnettuja operaatioita

3.1 Hyökkäys Ukrainan sähkönjakeluverkkoon 2015

Joulukuun 23. päivä vuonna 2015 Ukrainan sähkönjakeluverkkoon kohdistui kyberhyökkäys, joka aiheutti sähkökatkoksen jopa kuudeksi tunniksi yhteensä 225 000 asiakkaalle kolmen maakunnan alueella. Tämä hyökkäys on ensimmäinen julkisesti dokumentoitu onnistunut kyberhyökkäys sähkölaitoksen ohjausjärjestelmään. (Whitehead ym., 2017)

Hyökkäyksen taustalla epäillään olleen GRU:n Sandworm -nimellä tunnettu yksikkö 74455. Sandworm arvioitiin tekijäksi, koska sillä on ollut aiemminkin teknisten järjestelmien ohjauksessa käytettyihin SCADA-järjestelmiin (engl. Supervisory Control And Data Acquisition) Ukrainassa kohdistuneita operaatioita. Myös hyökkäyksessä käytetty haittaohjelma BlackEnergy 3 (BE3) on muodostunut heidän käyntikortikseen. (Hultquist, 2016)

Hyökkäys voidaan jakaa eri vaiheisiin riippuen katsontatavasta. Esimerkiksi Booz ym. (2016) jakaa hyökkäyksen 14 eri vaiheeseen. Whitehead ym. (2017) jakaa hyökkäyksen kahdeksaan eri vaiheeseen. Seuraavaksi tarkastellaan Whiteheadin esittämiä kahdeksaa vaihetta:

1. **Kohdennettu kalastelu:** Maaliskuussa 2015 hyökkääjät käyttivät kohdennettua kalastelumenetelmää (engl. spear phishing) saastuttaakseen laitteita, jonka avulla he pääsisivät kohdeverkkoihin. Hyökkääjät lähettivät uhreillensa

tiedostoja, jotka vaikuttivat tulleen Ukrainan energiaministeriöstä. Sähköpostiviestit sisälsivät Microsoft Exel -taulukon, tai Microsoft Word asiakirjan. Asiakirjan avaaminen ja makrojen käyttöönotto johti BE3:n asentamiseen kyseiselle tietokoneelle.

2. **Haittaohjelmien käyttäminen tutkimiseen ja verkossa liikkumiseen:** Saastuneen verkon tiedustelu ja kartoitus tapahtui useiden kuukausien ajan. Huhtikuussa 2015 hyökkääjät asensivat lisää takaovia saastuneille laitteille, jotka takasivat helpomman pääsyn saastuneisiin koneisiin. Ukrainan varaenergiaministerin mukaan oli todisteita, että hyökkääjät aloittivat verkkojen tiedustelun jopa kuusi kuukautta ennen hyökkäystä.
3. **Tunnistetietojen hankkiminen**: Yksi saastuneista tietokoneista oli sähköverkkoyhtiö Prykarpattiaoblenergon Active Directory – palvelin. Palvelin oli keskeinen tietoverkko infrastruktuurin kannalta ja se sisälsi käyttäjätunnuksia ja niiden salasanoja. Palvelimen murtautumistekniikkaa ei ole voitu varmentaa. Vaikka BE3:ssa on moduuli salasanojen varastamiselle, sen käytöstä ei jäänyt merkkejä.
4. **VPN-tunnelin luominen:** Hyökkääjät käyttivät varastettuja tunnistetietoja päästäkseen kohteen verkkoon. Hyökkääjät käyttivät kohteen VPN-yhteyttä käyttäjätunnuksilla ja salasanoilla, jotka he olivat aiemmin varastaneet. VPN-yhteyden avulla saatiin yhteys sähköverkkohallinnan HMI:hin (engl. Human-Machine Interface), käyttäen Remote Desktop -protokollaa (RDP), Remote Administrator (Radmin) etähallintaohjelmaa ja Secure Shelliä (SSH), jota käytetään salattuun tietoliikenteeseen.
5. **HMI-tietokoneisiin murtautuminen ja tiedustelu:** Pääsy yhteen Oblenergo-sähköyhtiön tietokoneista antoi valtuudet HMI-sovelluksen etäkäyttöön, joka mahdollisti hyökkääjille ohjausjärjestelmän etäkäytön. Ennen hyökkäystä hyökkääjät suorittivat tiedustelua ja murtautuivat ainakin 17 paikallisen jakelukeskuksen HMI-tietokoneelle, jotka ovat yhteydessä yli 50 sähköasemaan.
6. **Kytkinten ohjaaminen**: Hyökkäys alkoi kello 15:30, jatkui iskulla seuraavaan jakelukeskukseen minuuttia myöhemmin ja hyökkäys kolmanteen keskukseen alkoi noin kello 16:00. Sähköverkon operaattorit pystyivät vain katsomaan ja videomaan, kun hyökkääjät ottivat etäyhteyden ja avasivat katkaisijat yksi kerrallaan. Kello 16:10 yksi sähkölaitoksista poisti itse ylläpitäjän tilin käytöstä, mutta hyökkääjät jatkoivat toimintaa toisella pääkäyttäjätilillä. Myöhemmin sammutettiin koko SCADA-järjestelmä ja lopulta VPN. Hyökkäys kesti noin 60 minuuttia, ja lopulta operaattorit sammuttivat kaikki SCADA-järjestelmät ja siirtyivät manuaaliseen tilaan. Tämä oli ainoa tapa palauttaa sähköt. Yhdellä asemalla onnistuttiin ottamaan etäkäyttö pois päältä, mutta se pelasti vain yhden sähköaseman.
7. **Lisähyökkäykset:**
    a. **Palvelun estäminen puhelimitse:** Hyökkääjät käynnistivät TDoS-hyökkäyksen (engl. Telephony Denial of Service) häiritäkseen toimintoja ja sähköjen palauttamista Prykarpattiaoblenergossa ja Kyivoblenergossa. Puhelinkeskukset täyttyivät automatisoiduista ulkomaisista numeroista saapuvista puheluista. Tämä häiritsi yhtiöiden tilannekuvaa, koska vikailmoituspuhelut eivät tulleet läpi.
    b. **UPS:n etäkäyttö ja sammuttaminen:** Hyökkääjät käyttivät UPS:n (engl. Uninterruptible Power Supply) etähallintaliittymiä aikatauluttaakseen

tietokonepalvelimien sammuttamisen. Tällä pyrittiin todennäköisesti häiritsemään häiriötilanteen korjaus- ja palautustoimia.

c. **Haitallinen ohjelmistopäivitys:** Hyökkääjät lamauttivat tuntemattoman määrän sähköaseman tietoliikenneverkkolaitteita korruptoimalla niiden laiteohjelmiston. Valmistaja ei pystynyt korjaamaan kyseisiä laitteita.

8. **KillDiskin suorittaminen kohdetietokoneissa:** Hyökkääjät pyyhkivät joitain järjestelmiä KillDisk-haittaohjelman avulla hyökkäyksen päätteeksi. KillDisk poistaa valitut tiedostot kohdejärjestelmistään ja turmelee pääkäynnistystietueen, mikä tekee järjestelmän toimintakyvyttömäksi.

3.2 Demokraattien kansallisen komitean tietovuoto 2016

Vuosien 2015 ja 2016 aikana Yhdysvaltojen Demokraattisen puolueen kansallisen komitean (DNC) tietoverkkoon kohdistui kaksi erillistä tietomurtoa. Niiden tekijöiksi epäillään Cozy Bearia (APT29), joka usein yhdistetään joko FSB:hen, tai SVR:ään, sekä Fancy Bearia (APT28), joka yhdistetään GRU:hun (Nakashima & Harris, 2018).

Cozy Bearin tunkeutumisen on arvioitu tapahtuneen jo kesällä 2015, kun taas Fancy Bear murtautui DNC:n tietoverkkoon huhtikuussa 2016. Fancy Bearin ja Cozy Bearin tietomurrot ovat havaintojen mukaan olleet täysin erillisiä operaatioita, eikä ryhmien tiedetä tehneen yhteistyötä. (Alperovitsh, 2016)

3.2.1 Cozy Bearin suorittama tietomurto

Cozy Bearin hyökkäys perustui ensisijaisesti SeaDaddy -haittaohjelmaan, sekä Powershell -takaoveen, jonka pysyvyys toteutettiin Windows Management Instrumentation (WMI) -järjestelmän avulla. Sen avulla hyökkääjä saattoi käynnistää haitallista koodia automaattisesti tietyn ajanjakson jälkeen, tai tietyn aikataulun mukaisesti. Yksinkertainen Powershell-komento, joka on tallennettu vain WMI-tietokantaan, luo salatun yhteyden komento- ja valvontainfrastruktuuriin ja lataa sieltä lisää Powershell-moduuleja, jotka suoritetaan muistissa. Lisämoduulit voisivat teoriassa tehdä uhrin järjestelmässä mitä tahansa. Skriptin salausavaimet olivat jokaisessa järjestelmässä erilaiset. Toimijat käyttivät myös Powershell-versiota MimiKatz-työkalusta, jolla helpotettiin pääsyä järjestelmään. (Alperovitsh, 2016)

3.2.2 Fancy Bearin suorittama tietomurto

GRU:n yksiköiden 26165 (Fancy Bear) ja 74455 (Sandworm) epäillään toteuttaneen suurimman osan hyökkäyksestä DNC:n palvelimille. Yhden Fancy Bearin upseereista epäillään käyttäneen väärennettyjä henkilöllisyyksiä verkossa, kuten ”Den Katenberg” ja ”Yuliana Martynova”. Näitä nimiä käyttäen on lähetty kohdennettuja kalastelusähköposteja, joiden tarkoituksena on ollut huijata Clintonin vaalikampanjan henkilöstöä. Sähköposteissa oli linkki, jonka avaamalla hyökkääjät pystyivät saamaan uhrin kirjautumis- ja salasanatiedot. Toisen Fancy Bearin jäsenen epäillään kehittäneen X-Agent-haittaohjelman, jota käytettiin demokraattien kongressin kampanjakomitean ja DNC:n verkkojen hakkerointiin huhtikuussa 2016. Sandwormin epäillään järjestäneen varastettujen asiakirjojen julkaisun DCLeaks-nimisen verkkosivuston kautta nettipersoonalla Guccifer 2.0. (Nakashima & Harris, 2018)

Hyökkäys alkoi jo maaliskuussa 2016 kun John Podesta, Hilary Clintonin kampanjapäällikkö, sai kohdennetun kalastelusähköpostin. Sähköposti oli suunniteltu

näyttämään Googlen tietoturvailmoitukselta, joka kehotti käyttäjää vaihtamaan salasanan viestissä toimitetun linkin kautta. Podestan avustaja noudatti näitä ohjeita. Hyökkääjät pääsivät näin käsiksi kampanjapäällikön sähköpostitiliin ja sen sisältämiin yli 50 000 sähköpostiin. (Mueller, 2018)

Hyökkääjät jatkoivat kohdennettua kalastelua ja lähettivät kalastelusähköposteja useille tiedetysti Clintonin kampanjaan kuuluville henkilöille. Sähköpostit sisälsivät tiedoston, joka oli nimetty ”hillary-clinton-favorable-rating.xlsx.” Todellisuudessa tämä linkki ohjasi vastaanottajan hyökkääjän luomalle verkkosivulle. Saatuaan pääsyn demokraattisen puolueen kongressikampanjakomitean DCCC:n tietoverkkoon, hyökkääjät asensivat erilaisia haittaohjelmia, tiedustelivat verkkoa ja varastivat dataa. Käytettyjä haittaohjelmia olivat muun muassa erilaiset versiot hyökkääjien kehittämästä X-Agent haittaohjelmasta, joka mahdollisti yksittäisten henkilöiden toiminnan tarkkailun tietokoneella, salasanojen varastamisen ja DCCC:n tietoverkkoon pääsyn ylläpidon. (Mueller, 2018)

DCCC:n verkon kautta hyökkääjät loivat reitin DNC:n tietoverkkoon. Hyökkääjät asensivat useita haittaohjelmia DNC:n verkkoon samalla tavalla kuin DCCC:n verkkoon tiedustelun ja tiedostojen varastamista varten. Kun hyökkääjillä oli pääsy molempiin verkkoihin, he etsivät vuoden 2016 vaaleihin liittyviä avainsanoja, kopioivat DCCC:n kansioita ja kohdensivat toimiaan tietokoneisiin, jotka sisälsivät tietoa opposition tutkimuksesta ja kenttäoperaatiosuunnitelmista vuoden 2016 vaaleja varten. (Mueller, 2018)

Hyökkääjät käyttivät varastetun datan siirtämiseen toista kehittämäänsä haittaohjelmaa X-Tunnelia. X-Tunnel-verkkotunnelointityökalu helpottaa yhteyksiä osoitteenmuunnoksiin käytettyihin NAT-ympäristöihin ja sitä käytettiin myös etäkomentojen suorittamiseen. Työkalua käytettiin RemCOM:in kautta. Lisäksi hyökkääjät käyttivät useita rikosteknisen analyysin vastaisia toimenpiteitä, joilla ajoittain tyhjennettiin tapahtumalokeja ja nollattiin tiedostojen aikaleimoja. (Alperovitsh, 2016)

Lopulta hyökkääjät jakoivat varastamiaan sähköposteja ja tiedostoja WikiLeaksille. WikiLeaks julkaisi arkiston DNC:n sähköposteista, joka sisälsi yli 20000 sähköpostia ja muuta dokumenttia. (Nakashima & Harris, 2018)

3.2.3 FBI:n varoitus tietomurrosta

FBI varoitti DNC:tä ensimmäisen kerran hyökkäyksen kohteeksi joutumisesta syyskuussa 2015. Asiantuntija tarkasti tietoverkon, eikä löytänyt järjestelmästä mitään erikoista. FBI varoitti DNC:tä uudestaan marraskuussa 2015, jolloin tuli ilmi, että verkon tarkastanut henkilö ei koskaan ilmoittanut havaitusta tietomurrosta eteenpäin. Huhtikuussa 2016 verkkoon alkoi ilmestyä tasaiseen tahtiin DNC:n sähköposteista varastettuja tietoja, ja 12.6.2016 WikiLeaksin perustaja Julian Assange ilmoitti julkaisevansa tietomurrossa varastetut tiedot WikiLeaksin sivuilla. Kolme päivää Assangen ilmoituksen jälkeen tietoturvayhtiö Crowdstrike, jonka DNC oli palkannut selvittämään ja paikkaamaan tietomurtoa, julkaisi selvityksen hyökkäyksistä, jossa se nimesi hyökkääjiksi Fancy Bearin ja Cozy Bearin. (CNN, 2022)

4 Kyberoperaatioiden tavoitteet

Venäjän tiedustelupalveluiden toteuttamien kyberoperaatioiden tavoitteita ei ole yksiselitteistä selvittää. Tämä johtuu osaksi tiedustelupalveluiden pyrkimyksestä toimia

salassa ja osaksi kyberympäristön ominaispiirteistä, jotka tekevät hyökkäyksen attribuutiosta vaikeaa (Greenberg, 2019). Vaikka tavoitteita on vaikea määritellä, ovat asiantuntijat spekuloineet operaatioiden tavoitteita arvioimalla muun muassa operaatioissa tehtyjä toimenpiteitä niitä ympäröivässä kontekstissa.

4.1.1 Sabotaasi infrastruktuuria kohtaan

GRU:hun liitetyn Sandworm-ryhmän tekemät iskut Ukrainan sähköverkkoa vastaan ovat malliesimerkki kyberoperaatiosta, jossa mitä ilmeisimpänä tavoitteena on ollut sabotaasi. Ryhmän iskuissa vuosina 2015 ja 2016 hyökättiin sähköinfrastruktuuria vastaan. Useiden sähköyhtiöiden sähköasemiin ja muuntaja-asemiin hyökättiin ja aiheutettiin sähkökatkot, jotka koskettivat tuhansia ihmisiä. Varsinaista motiivia sabotaasin takana on vaikea arvioida. Eri asiantuntijat ovat arvioineet, että hyökkääjät olisivat voineet aiheuttaa pahempiakin vahinkoja erityisesti vuoden 2016 iskun aikana. Tämä on johtanut asiantuntijoiden spekulaatioon siitä, oliko hyökkäyksien motiivina kyvykkyyksien testaaminen, lännen tai Ukrainan pelottelu, lännen vastauksen testaaminen vai poliittisen tason viestin lähettäminen lännelle ja Ukrainalle. (Greenberg, 2019)

4.1.2 Tietojen kerääminen

Vuosina 2015 ja 2016 Yhdysvaltain demokraattisen puolueen kansallinen komitea (DNC) oli kahden eri Venäjän tiedustelupalveluihin liitetyn ryhmän hyökkäysten kohteena. Näiden hyökkäyksien ilmeisimpänä tavoitteena on ollut tietojen kerääminen. Kerättyjä tietoja vuodettiin Wikileaksin sekä GRU:hun liitetyn ryhmän, ”Fancy Bearin”, luoman nettisivun kautta. (Lipton, Sanger, & Shane, 2016)

Eri tahot ovat arvioineet hyökkäyksien olleen tapa heikentää uskoa Yhdysvaltojen demokratiaan, mustamaalata Hillary Clinton, heikentää hänen mahdollisuuksiaan tulla valituksi presidentiksi sekä parantaa Donald Trumpin mahdollisuuksia presidentinvaaleissa. (Office of the Director of National Intelligence, 2017; United States Senate, 2019). Fancy Bear on nimetty kerättyjen tietojen vuotajaksi. SVR:ään liitetty ryhmä, ”Cozy Bear”, on tunnettu lähinnä tiedon keräämisestä, ei tietojen julkaisusta. Tämän vuoksi onkin arvioitu, että Cozy Bearin tavoitteena tässäkin operaatiossa oli ainoastaan tiedon kerääminen. (F-Secure, 2015, 2020; Mueller, 2019)

4.1.3 Sotilasoperaatioiden tukeminen

Jo hieman ennen Georgian ja Venäjän välistä sotaa elokuussa 2008, Georgian internet -infrastruktuuria vastaan hyökättiin verkon kautta (Markoff, 2008). Varsinaisen sodan alkaessa kyberhyökkäykset jatkuivat ja niistä tuli entistä koordinoidumpia. Kyberhyökkäykset kohdistuivat tiettyihin kaupunkeihin juuri ennen niiden pommituksia. Hyökkäykset myös loppuivat samalla kun venäläiset aloittivat tulitaukoneuvottelut. Osa hyökkääjistä käytti samoja työkaluja, joita Sandworm-ryhmä käytti myöhemmin. Georgian kyberhyökkäyksiä ei tosin ole suoraan liitetty Venäjään tai sen tiedustelupalveluihin. (Greenberg, 2019)

Myös vuonna 2022 Venäjän Ukrainaan aloittaman täysimittaisen hyökkäyksen alkaessa Ukrainaan kohdistui useita kyberhyökkäyksiä. Osa näistä hyökkäyksistä on liitetty aiemmin mainittuun Sandworm-ryhmään. Näissä operaatioissa käytettiin palvelunestohyökkäyksiä sekä useita erilaisia datan tuhoamiseen tarkoitettuja ”wiper” -haittaohjelmia ja uutta versiota Sandwormin vuonna 2016 käyttämästä Industroyer-

haittaohjelmasta. (Cherepanov & Lipovsky, 2022.) Ensimmäinen kyberhyökkäyksistä tapahtui vain tunteja ennen Venäjän aloittamaa sotilaallista hyökkäystä. Tässä hyökkäyksessä käytetty haittaohjelma oli aikaleiman perusteella luotu 28.12.2021 eli hyvissä ajoin ennen hyökkäystä. Huhtikuussa 2022 Ukrainan CERT (engl. Computer Emergency Response Team) -viranomainen tiedotti Sandworm-ryhmän kyberhyökkäyksestä, jolla oli tarkoitus aiheuttaa sähkökatko iskemällä Ukrainan kriittiseen sähköinfrastruktuuriin. (CERT-UA, 2022.) Vuoden 2022 aikana Venäjä on pyrkinyt tukemaan aseellista hyökkäystä erilaisilla kyberhyökkäyksillä (Burt, 2022).

4.1.4 Poliittisen viestin lähettäminen

Vuoden 2018 talviolympialaisten avajaisten alkaessa olympialaisten järjestäjät huomasivat ongelmia tietojärjestelmissään. Olympialaisten alkaessa IT-infrastruktuurin kriittisimmät palvelimet sammuivat. Tämän hyökkäyksen takana oli haittaohjelma, jolle annettiin nimi ”Olympic destroyer”. Se sisälsi paljon harhaanjohtavia vihjeitä sen tekijästä. Haittaohjelma sisälsi linkkejä Pohjois-Koreaan sekä Kiinaan liitettyihin hakkeriryhmiin. Viitteet olivat kuitenkin todistettavasti harhauttavia, ja useat asiantuntijat liittivät nämä hyökkäykset yleisesti Venäjän valtioon, ja erityisesti Sandworm-ryhmään. (Greenberg, 2019; Nakashima, 2018.) Asiantuntijat ovat arvioineet hyökkäyksien olevan kosto Venäjän sulkemisesta olympialaisten ulkopuolelle dopingskandaalin takia (Greenberg, 2019; Mercer, Rascagneres, Baker, & Molyett, 2018).

5 Johtopäätökset

5.1 Arvioita Venäjän kyberoperaatioista

Venäjän tiedustelupalveluihin ja erityisesti niiden toimintaan kyberympäristössä liittyy erityispiirteitä, jotka tekevät niiden seuraamisesta erityisen vaikeaa. On kuitenkin selvää, että tiedustelupalveluiden tekemät kyberoperaatiot ovat todellisia. Esimerkiksi Suojelupoliisi totesi vuoden 2020 olleen vakoilun alalla kybervakoilun vuosi (Suojelupoliisi, 2020). Tiedustelutoimintaa kyberoperaatioiden avulla on havaittu Suomessakin. Esimerkiksi vuonna 2013 Venäjän FSB:hen liitetty ryhmä ”Turla” onnistui murtautumaan Ulkoministeriön järjestelmiin (YLE, 2016).

Myös Venäjän muihin tiedustelupalveluihin liitetyt ryhmät ovat aktiivisia kyberympäristössä. FSB:n lisäksi GRU:hun ja SVR:ään liitetyt ryhmät ovat olleet asiantuntijoiden mukaan useiden erilaisten kyberoperaatioiden takana. Vaikka nämä ryhmät ovat toteuttaneet myös fyysiseen ympäristöön vaikuttavia kyberiskuja, on valtaosa julkisuuteen tulleista operaatioista ollut tiedustelupalveluille tyypillisiä arkaluontoisten tietojen keräämistä. (Council on Foreign Relations, 2022).

Tiedustelupalveluihin liitetyt ryhmät eivät ole kuitenkaan tyytyneet ainoastaan keräämään tietoja. Asiantuntijoiden mukaan kyberoperaatioilla on yritetty muun muassa tukea sotilasoperaatioita, lähettää erilaisia poliittisia viestejä ja signaaleja, häiritä vaaleja sekä pelotella. Osa näistä tavoitteista on mitä ilmeisimmin saavutettu. Esimerkiksi entinen Yhdysvaltain kansallisen turvallisuusviraston (NSA) ja keskustiedustelupalvelun (CIA) johtaja joutui myöntämään vuoden 2016 presidentinvaaleihin vaikuttaminen olleen ”historian onnistunein salainen operaatio” (Munslow, 2017). Myös todella monet vakoiluoperaatiot ovat kestäneet vuosia, joten voitaneen olettaa ainakin joidenkin niistä olleen onnistuneita.

Jos verrataan viime vuosien hyökkäyksiä vuonna 2007 Viroon kohdistuneisiin palvelunestohyökkäyksiin, ovat hyökkäykset muuttuneet epäilemättä kehittyneemmiksi. Toisaalta, jos verrataan viime vuosien hyökkäyksiä ensimmäiseen julkisesti Venäjään liitettyyn APT-hyökkäykseen, jossa jo vuonna 1996 on onnistuttu varastamaan Yhdysvalloilta salaisia tietoja kyberoperaatiolla, ovat Venäjän tiedustelupalveluihin liitettyjen ryhmien tekemät kyberoperaatiot usein silti perusperiaatteeltaan vieläkin samanlaisia (Pankov, 2017). Edelleen useimmissa operaatioissa tavoitteena ja toimintaperiaatteena on saada tietomurroilla pääsy salaiseen tietoon ja varastaa tietoja. Vaikka tekniikat ja teknologiat ovat kehittyneet merkittävästi viimeisen 20-vuoden aikana, tiedustelun merkitys on edelleen keskeinen.

5.2 Esitykset jatkotutkimuksesta

Tutkimuksen arvoista voisi olla selvittää miksi vuonna 2022 Venäjän sotilaallista hyökkäystä tukemaan tehdyt kyberoperaatiot eivät saavuttaneet läheskään yhtä isoja vaikutuksia kuin sähköinfrastruktuuria vastaan tehdyt iskut vuosina 2015 ja 2016 tai vuoden 2017 NotPetya-hyökkäys. Voiko syynä olla yksinkertaisesti Ukrainan kyberturvallisuuden kehittyminen vuosien aikana? Entä voiko syynä olla, että myöskään Venäjän tiedustelupalvelut eivät uskoneet Vladimir Putinin päättävän aloittaa hyökkäystä, ja tästä syystä ne eivät ehtineet valmistautua kyberhyökkäyksiin? Tai voisiko syynä olla Yhdysvaltain Ukrainalle antama tiedusteluapu, jolla kyberhyökkäyksiin on pystytty varautumaan?

Jatkotutkimukseksi esitämme Venäjän tiedustelupalveluiden kybertoiminnan vertaamista muihin merkittävien maiden, kuten Yhdysvaltojen ja Kiinan kyberkyvykkyyteen ja -toimintaan. Myös koska näiden operaatioiden tutkiminen on hankalaa, olisi mielenkiintoista mahdollisesti tulevaisuudessa päästä tutkimaan näiden tiedustelupalveluiden arkistoja. Näin olisi mahdollista saada parempi kuva näiden kyberympäristössä toimivien ryhmien toiminnasta, kyvyistä sekä esimerkiksi taktiikoista.

Lähteet

Alperovitsh, D. (2016). CrowdStrike_BearsintheMidst_DNC(06-04-2016). *Crowdstrike*. Haettu 15.11.2022 osoitteesta: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Bagge, D. P. (2019). *Unmasking Maskirovka: Russia's Cyber Influence Operations*. Defense Press.

Burt, T. (2022, April 27). The hybrid war in Ukraine. Haettu 10.11.2022 osoitteesta: https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/

CERT-UA. (2022, December 4). Кібератака групи Sandworm (UAC-0082) на об'єкти енергетики України з використанням шкідливих програм INDUSTROYER2 та CADDYWIPER (CERT-UA#4435). Haettu 6.11.2022: https://cert.gov.ua/article/39518

Cherepanov, A., & Lipovsky, R. (2022). *Sandworm's Cyberwarfare Targets Ukraine's Power Grid Again*. Haettu 15.11.2022 osoitteesta: https://i.blackhat.com/USA-22/Wednesday/US-22-Cherepanov-Industroyer2-Sandworms-Cyberwarfare-Targets-Ukraines-Power-Grid-Again.pdf

CNN Editorial Research. (2022, October 20). *2016 Presidential Campaign Hacking Fast Facts*. Haettu 15.11.2022 osoitteesta: https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html

Council on Foreign Relations. (2022). Tracking State-Sponsored Cyberattacks Around the World. Haettu 10.11.2022 osoitteesta: https://www.cfr.org/cyber-operations

Congressional Research Service (2021). Cybersecurity: Selected Cyberattacks, 2012–2021. Haettu 12.11.2022 osoitteesta: https://crsreports.congress.gov/product/pdf/R/R46974

Congressional Research Service (2022). Russian Cyber units. Haettu 12.11.2022 osoitteesta: https://crsreports.congress.gov/product/pdf/IF/IF11718

Council on Foreign Relations. (2022). Tracking State-Sponsored Cyberattacks around the World. Haettu 11.11.2022 osoitteesta: https://www.cfr.org/cyber-operations

F-Secure. (2015). *The Dukes 7 Years Of Russian Cyberespionage*. Haettu 15.11.2022 osoitteesta: https://blog.f-secure.com/wp-content/uploads/2020/03/F-Secure_Dukes_Whitepaper.pdf

F-Secure. (2020, May 6). 039| Deconstructing the Dukes: A Researcher's Retrospective of APT29. Haettu 9.11.2022 osoitteesta: https://blog.f-secure.com/podcast-dukes-apt29/

Greenberg, A. (2019). *Sandworm*. Doubleday.

Hultquist, J. (2016, August 23). *Sandworm Team and the Ukrainian Power Authority Attacks | Mandiant*. Haettu 15.11.2022 osoitteesta: https://www.mandiant.com/resources/blog/ukraine-and-sandworm-team

Lilly, B., & Cheravitch, J. (2020). The Past, Present, and Future of Russia's Cyber Strategy and Forces. *2020 12th International Conference on Cyber Conflict (CyCon)*, 129–155. Estonia: IEEE. Haettu 15.11.2022 osoitteesta: https://doi.org/10.23919/CyCon49761.2020.9131723

Lipton, E., Sanger, D. E., & Shane, S. (2016, December 13). The Perfect Weapon: How Russian Cyberpower Invaded the U.S. *The New York Times*. Haettu 15.11.2022 osoitteesta: https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

Markoff, J. (2008, August 12). Before the Gunfire, Cyberattacks. *The New York Times*. Haettu 15.11.2022 osoitteesta: https://www.nytimes.com/2008/08/13/technology/13cyber.html

Mercer, W., Rascagneres, P., Baker, B., & Molyett, M. (2018, February 12). Olympic Destroyer Takes Aim At Winter Olympics. Haettu 9.11.2022 osoitteesta: https://blog.talosintelligence.com/olympic-destroyer/

Mueller, R. S. (2019). Report on the Investigation into Russian Interference in the 2016 Presidential Election (p. 448). Haettu 15.11.2022 osoitteesta: https://www.justice.gov/archives/sco/file/1373816/download

Mueller, R.S. (2018). *Case 1:18-cr-00215-ABJ*. Haettu 15.11.2022 osoitteesta: https://www.justice.gov/file/1080281/download

Munslow, J. (2017, July 22). Ex-CIA Director Hayden: Russia election meddling was 'most successful covert operation in history.' Haettu 10.11.2022 osoitteesta: https://www.yahoo.com/news/ex-cia-director-hayden-russia-election-meddling-successful-covert-operation-history-212056443.html

Nakashima, E. (2018, February 26). Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say. *Washington Post*. Haettu 15.11.2022 osoitteesta: https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html

Nakashima, E., & Harris, S. (2018, July 13). *How the Russians hacked the DNC and passed its emails to WikiLeaks - The Washington Post*. The Washington Post. Haettu 15.11.2022 osoitteesta: https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html

Office of the Director of National Intelligence. (2017). *Assessing Russian Activities and Intentions in Recent US Elections*.

Pankov, N. (2017, April 3). Moonlight Maze: Lessons from history. Haettu 15.11.2022 osoitteesta:https://www.kaspersky.com/blog/moonlight-maze-the-lessons/6713/

Pihlak, H. (2018, October 16). NATO CCDCOE - Expertise and cooperation make our cyber space safer. Haettu 6.11.2022 osoitteesta: https://e-estonia.com/nato-ccdcoe-expertise-cyber-space-safer/

Suojelupoliisi. (2020). *Suojelupoliisi vuosikirja 2020*. Haettu 15.11.2022 osoitteesta: https://supo.fi/documents/38197657/40760236/Supo+Vuosikirja+2020.pdf/70e75573-0726-f76c-846c-be661887c9db/Supo+Vuosikirja+2020.pdf?t=1646741936184

The Center for European Policy Analysis(2022). Russian Cyberwarfare: Unpacking the Kremlin's Capabilities. Haettu 12.11.2022 osoitteesta: https://cepa.org/wp-content/uploads/2022/09/Unpacking-Russian-Cyber-Operations-9.2.22.pdf

The Cybersecurity and Infrastructure Security Agency (2016). GRIZZLY STEPPE – Russian Malicious Cyber Activity. Haettu 12.11.2022 osoitteesta: https://www.cisa.gov/uscert/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

The Cybersecurity and Infrastructure Security Agency (2021). Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders. Haettu 12.11.2022 osoitteesta: https://www.cisa.gov/uscert/ncas/alerts/aa21-116a

The Cybersecurity and Infrastructure Security Agency (2022). Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. Haettu 12.11.2022 osoitteesta: https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

The Department of Justice (2017). U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts. Haettu 12.11.2022 osoitteesta: https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions

The Department of Justice (2018). Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election. Haettu 12.11.2022 osoitteesta: https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

The Department of Justice (2018). Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace. Haettu 12.11.2022 osoitteesta: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

The Foreign, Commonwealth & Development Office (2022). Russia's FSB malign activity: factsheet. Haettu 12.11.2022 osoitteesta: https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet

The National Cyber Security Centre (2021). Joint advisory: Further TTPs associated with SVR cyber actors. Haettu 15.11.2022 osoitteesta: https://www.ncsc.gov.uk/news/joint-advisory-further-ttps-associated-with-svr-cyber-actors

The Warsaw Institute (2020). Welcome to Cyberwar. Haettu 12.11.2022 osoitteesta: https://warsawinstitute.org/welcome-to-cyberwar/

United States Senate, S. C. on I. (2019). *Russian Active Measures Campaigns and Interference In The 2016 U.S Election—Volume 5*. Haettu 15.11.2022 osoitteesta: https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf

U.S. Department of Defense (2022). Joint Cybersecurity Advisory. Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. Haettu 11.11.2022 osoitteesta: https://media.defense.gov/2022/Apr/20/2002980529/-1/-1/1/JOINT_CSA_RUSSIAN_STATE-SPONSORED_AND_CRIMINAL_CYBER_THREATS_TO_CRITICAL_INFRASTRUCTURE_20220420.PDF

U.S. Department of State (2020). The United States Condemns Russian Cyber Attack Against the Country of Georgia. Haettu 12.11.2022 osoitteesta: https://2017-2021.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/index.html

Whitehead, D. E., Owens, K., Gammel, D., & Smith, J. (2017, October 30). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. *70th*

Annual Conference for Protective Relay Engineers, CPRE 2017. Haettu 15.11.2022 osoitteesta: https://doi.org/10.1109/CPRE.2017.8090056

YLE. (2016, January 13). Russian group behind 2013 Foreign Ministry hack. Haettu 10.11.2022 osoitteesta: https://yle.fi/uutiset/osasto/news/russian_group_behind_2013_foreign_ministry_hack/8591548

TIEDUSTELUN KÄYTTÖ INFORMAATIOVAIKUTTAMISEN VÄLINEENÄ VENÄJÄN-UKRAINAN SODASSA

Kateřina Buchtová, Markus Kallatsa, Säde Latikka, ym.

1 Johdanto

Helmikuussa 2014 Ukrainan vallankumouksen jälkeen alkoi vielä tämän raportin kirjoitushetkelläkin käynnissä oleva sota Venäjän ja Ukrainan välillä. Sodan alkuvaiheessa Venäjä toteutti Krimin valtaamisen. Myöhemmin Itä-Ukrainassa käynnistyi sota, joissa osapuolina olivat Ukraina ja Venäjän tukemat separatistit. Venäjä keskitti Itä-Ukrainaan myös omia joukkojaan. Sota laajeni Venäjän aloittaessa laajamittaisen hyökkäyksen Ukrainaan helmikuussa 2022.

Nykyaikainen sodankäynti poikkeaa historiallisista sodista muun muassa teknisen kehityksen myötä, mikä näkyy esimerkiksi tietoverkkojen kautta tapahtuvassa viestinnässä. Vaikuttaminen liittyy läheisesti viestintään. Tällöin voidaan puhua informaatiovaikuttamisesta. Tässä raportissa tarkastellaan Venäjä-Ukrainan sodan tapahtumia informaatiovaikuttamisen näkökulmasta. Tarkastelu keskittyy ajallisesti helmikuun 2022 jälkeiselle ajanjaksolle.

Informaatiovaikuttamisella on Venäjällä pitkät perinteet ja se käsittää paljon erilaisia toimia, kuten kyber- ja psykologisia operaatioita, strategista viestintää tai maskirovkaa (harhauttamista). Venäjä pyrkii informaatiovaikuttamisella heikentämään, hämmentämään ja horjuttamaan vastustajiaan. Venäjä on tässä sodassa pyrkinyt vaikuttamaan kotiyleisöön, ukrainalaisiin, länsimaihin sekä kolmansiin maihin. Venäjän tiedustelupalveluilla on informaatiovaikuttamisessa keskeinen rooli.

Venäjän-Ukrainan sodan aikana Ukraina on harjoittanut ja ylläpitänyt vahvaa sisäistä viestintää, mutta myös laajaa ulkoiseen propagandaan rinnastettavaa viestintää. Tavoitteena on ollut saada julkista tukea ja korostaa Ukrainan sotatoimien menestystä. Viestinnällä on ollut Ukrainan lisäksi erityisesti Euroopassa ja Yhdysvalloissa merkittävä vaikutus. Välineinä Ukraina on käyttänyt perinteisiä uutiskanavia, mutta myös sosiaalista mediaa, kuten Youtube- ja TikTok-videoita ja muita verkkomedioita.

Yhdysvallat ja Iso-Britannia ovat omassa informaatiovaikuttamisessaan pyrkineet kumoamaan valeuutisia, sekä levittämään paikkaansa pitävää tietoa vastatakseen Venäjän informaatiosodankäyntiin. Ennen hyökkäyksen alkua syksyllä 2021, Yhdysvallat ja Iso-Britannia paljastivat Venäjän suunnitelmia, kuten erilaisia false-flag-operaatioita, sekä antoivat hyökkäyksestä ennakkovaroituksen.

Raportin alkuosassa käsitellään informaatiovaikuttamisen käsitettä ja sen yhteyttä tiedusteluun, erityisesti median näkökulmasta. Loppuosa painottuu eri maiden informaatiovaikuttamisen tapauksiin. Venäjän-Ukrainan sodan osapuolten informaatiovaikuttamista käsitellään luvuissa 3 (Venäjä) ja 4 (Ukraina). Yhdysvaltojen ja Iso-Britannian informaatiovaikuttamista käsitellään raportin luvuissa 5 ja 6. Raportin lopussa on esitelty lähdeaineiston perusteella laaditut johtopäätökset.

2 Informaatiovaikuttaminen ja tiedustelu

2.1 Informaatiovaikuttaminen

Viestintää voidaan toteuttaa useassa eri ulottuvuudessa. Keskustelun käymiseen on luotu monia eri alustoja, jotka mahdollistavat tiedon välittämisen maailmanlaajuisesti. Demokratia voi synnyttää avointa keskustelua, jossa esille nousee erilaisia mielipiteitä ja vaikuttamiskampanjoita. Keskusteluun osallistuvia osapuolia ovat niin yksittäiset kansalaiset kuin kansalaisyhteiskunnan edustajatkin. Viestinnän merkitys on myös korostunut Venäjän-Ukrainan sodassa, jossa viestintää on käytetty informaatiovaikuttamisen keinona.

Viestinnän roolin kasvaessa eräs huomionarvoinen seikka on sisällön todenmukaisuus. Valeuutisointia toteutetaan tyypillisesti sosiaalisen median avulla perinteisen valtavirtamedian sijaan (Balmas, 2014). Yksilöiden ja ryhmien näkökulmasta sosiaalista mediaa voidaan hyödyntää väärän tiedon tahallisessa tai tahattomassa levittämisessä. Edellä kuvatun toimintamallin eräs huono puoli on se, että hallitusten, yritysten ja kansalaisten mahdollisuudet puuttua valheellisen tiedon levittämiseen ovat vaikeutuneet (Napper, 2020).

Valtioneuvoston kanslian tuottamassa viestijöille suunnatussa oppaassa nostetaan esille valeuutisoinnin myötä havaittuja viestinnän haavoittuvuuksia, joita erilaiset toimijat käyttävät hyväkseen informaatiovaikuttamisessa (VNK, 2019). Oppaassa informaatiovaikuttaminen määritellään toimintana, jonka tavoitteena on vaikuttaa järjestelmällisesti yleiseen mielipiteeseen, ihmisten käyttäytymiseen ja päätöksentekijöihin. Vaikuttaminen voi lopulta heijastua yhteiskunnan toimintakykyyn. Informaatiovaikuttaminen voidaan määritellä myös sodankäynnin näkökulmasta. Fogleman ja Widnal (1997) määrittelevät informaatiovaikuttamisen *informaatiotoimina*, joilla kielletään, hyödynnetään, turmellaan tai tuhotaan vihollisen tietoja ja informaatiotoimia, sekä suojaudutaan vihollisen informaatiotoimilta ja hyödynnetään omia sotilaallisia informaatiotoimia. Kirjoittajat ovat määritelleet informaatiotoimen toimintana, johon liittyy tiedon hankkimista, siirtämistä, tallentamista tai muuntamista. Informaatiovaikuttamisen määritelmä ei siis ole yksiselitteinen, mutta useimmat niistä liittyvät kuitenkin muutoksen aikaansaamiseen viestinnän avulla.

2.2 Tiedustelu ja viestintä sodankäynnissä

Perinteinen ajatus sodankäynnistä liittyy aseellisten eli kineettisten suorituskykyjen käyttöön fyysisessä ympäristössä. Digitalisoituneessa ja verkottuneessa maailmassa viestinnän kasvanut merkitys heijastuu myös sodankäyntiin. Tietoverkot mahdollistavat tiedonvälityksen eri tavoilla. Ei-kineettiseen suorituskykyyn luetaan mukaan myös perinteinen viestintä, kuten televisio ja painetut lehdet. Olennainen ero verkottuneessa maailmassa on kuitenkin se, että tiedon rooli voi olla yhtä merkittävä kuin kineettisen vaikuttamisen, ellei jopa merkittävämpi. (Farwell, 2020).

Tieto vastustajasta ja sen toiminnasta ovat edellytys suunnittelulle, varautumiselle ja tehokkaille vastatoimille. *Tiedustelulle* ei ole olemassa vakiintunutta ja yksiselitteistä määritelmää, mutta se voidaan yleisesti nähdä prosessina, joka alkaa asiakkaan tietopyynnöstä jatkuen tiedonkeräyksen ja -käsittelyn jälkeen jakeluvaiheeseen. Tietoa kerätään eri menetelmillä, joista kehittyneimmät ovat osin automatisoituja (Pelletie, 2022).

Tiedustelun avulla tuotetun tiedon oletetaan olevan neutraalia. Tiedustelun ei itsessään pitäisi ottaa kantaa päätöksentekoprosessiin, vaan tuottaa tietoa päätöksenteon tueksi. On kuitenkin havaittu, että tiedustelutietoa tuottavat analyytikot ovat vääristäneet tiedustelutuotteita vaikuttamistarkoituksessa (Bollfrass, 2017). Sen lisäksi, että vääristynyttä tiedustelutietoa käytetään päätöksenteossa, voidaan tiedustelun avulla kerättyä tietoa julkaista mediassa osana informaatiovaikuttamista.

2.3 Tiedustelutiedon julkaiseminen

Toinen maailmansota ja erityisesti kylmän sodan loppupuoli ovat olleet ajanjaksoja, jolloin media on julkaissut huomattavan paljon tiedusteluaiheisia uutisia. Tiedusteluun liittyvät julkaisut skandaaleista ja paljastuksista ovat lisänneet ihmisten kiinnostusta aiheeseen, ja samalla kasvattaneet tiedusteluaiheisten julkaisujen suosiota mediassa (Teirilä, 2016).

Median motiivina tiedustelutiedon julkaisemiseen voi olla tiedustelutiedon salainen luonne, joka voi kiehtoa sen lukijakuntaa. Tiedustelupalveluiden salamyhkäisyyden vuoksi suuri yleisö voi haluta tietoja mahdollisista väärinkäytöksistä. Tällöin tiedotusvälineet täyttävät demokraattisen vastuun tuodessaan niitä esille (Shpiro, 2001).

Julkaistut tiedustelutiedot voivat olla peräisin esimerkiksi tietovuodoista, tyytymättömiltä työntekijöiltä tai tuloksena pelkästä spekulaatiosta (Shpiro, 2001). Tietojen julkaisemiseen on käytössä useita eri alustoja. Perinteisen painetun median, television ja radion lisäksi hyödynnettävissä on myös internet, erityisesti sen sosiaalisen median palvelut. Esimerkiksi Venäjä käyttää kyberavaruus -termin sijaan termiä informaatioavaruus. Siihen lasketaan mukaan sekä tietokoneen että ihmisen suorittama informaation prosessointi (Akimenko ym., 2020).

Hillebrand (2012) on määritellyt medialle kolme roolia tiedustelun valvonnassa:

1. Media toimii välittäjänä ja virikkeenä muodollisille tarkastajille.
2. Media toimii korvaavana ”vahtikoirana”.
3. Media toimii legitimoivana instituutiona.

Ensimmäinen ja yleisin rooli on tutkia ja välittää tietoa hallitusten ja muiden tahojen toimista, myös tiedustelupalveluja koskien. Median kautta tiedustelua koskevat aiheet voivat nousta julkiseen keskusteluun. Tiedustelutoiminnan osalta tämä voi tarkoittaa muun muassa mahdollisten ihmisoikeusloukkausten, toimivaltuuksien väärinkäytösten ja toiminnan puutteiden esille nostamista. Tiedotusvälineiden oletetaan punnitsevan huolellisesti julkaisuista mahdollisesti aiheutuvia haittoja. Aineistosta saatetaan käydä epävirallisia keskusteluja virkamiesten kanssa.

Toinen rooli liittyy valvonnan mahdollisten aukkojen täyttämiseen. Jos yksityishenkilöt kokevat syystä tai toisesta, etteivät he voi lähestyä virallisia tiedustelun valvonnasta vastaavia toimijoita tai ne eivät ole huomioineet jotain ongelmaa, media olla vaihtoehtoinen yhteydenoton taho. Myös oppositiopoliitikot voivat hyödyntää median vaikutusta herättäessään kiinnostuksen jotain tiettyä aihetta tai puutetta kohtaan, erityisesti mikäli taustalla on esimerkiksi viranomaisten väärinkäytöksiä.

Kolmas rooli liittyy tiedustelutoiminnan legitimoimiseen. Tiedottamalla yleisölle tiedustelupalvelujen toiminnasta ja politiikasta, voidaan edesauttaa luottamuksen rakentumista näitä instituutioita kohtaan, ja osoittaa että tiedustelutoimintaa valvotaan riippumattomasti. Luottamus liittyy olennaisesti tilanteisiin, joissa tiedustelupalvelut

joutuvat ehkä turvautumaan yleisön tukeen ja yhteistyöhön. Luottamus ja hyväksyntä ovat myös eduksi, kun keskustellaan budjetista ja mahdollisista toimivaltuuksien laajentamisesta.

3 Venäjä

Venäjällä informaatiovaikuttaminen ja -sota ymmärretään konseptina, joka kattaa laajan kirjon toimintatapoja, kuten tietoverkko-operaatioita, psykologisia operaatioita, strategista viestintää, maskirovkaa, disinformaatiota ja elektronista sodankäyntiä (Giles, 2016). Venäjällä informaatiovaikuttaminen jakaantuu informaatiotekniseen osaan, jonka kohteena ovat informaatiotekniset järjestelmät (sanomalehdet, televisio, sosiaalisen median palvelut), ja informaatiopsykologiseen osaan, jonka kohteena ovat ihmismieli ja yhteiskunnan kyky tehdä päätöksiä (Kari, 2022). Venäjän tiedustelu- ja turvallisuuspalvelujen osallistumista informaatiovaikuttamiseen on ollut aiemmin vaikea vahvistaa. Viime vuosina on kuitenkin tullut ilmi yhä enemmän todisteita palvelujen aktiivisesta roolista (Pynnöniemi, 2019).

Venäjän hallituksen ja muiden venäläisten toimijoiden systemaattisesti harjoittama tiedon manipulointi ja disinformaatio ovat osa Venäjän-Ukrainan sodan operatiivisia työkaluja. Kyse ei ole uudesta ilmiöstä, vaan jatkumosta Venäjän pitkäaikaiselle informaatiovaikuttamiselle demokraattisia yhteiskuntia vastaan. Venäjä pyrkii heikentämään, hämmentämään ja horjuttamaan vastustajiaan (OECD, 2022). Disinformaation levittämisellä ja strategisella harhauttamisella on Venäjällä jo satavuotiset perinteet (Kari, 2022).

Venäjän tiedustelu- ja turvallisuuspalvelujen informaatiovaikuttamisoperaatiot kohdistuvat Venäjän-Ukrainan sodassa neljään eri kohderyhmään: venäläisiin, ukrainalaisiin, länsimaihin ja kolmansien maiden kansalaisiin. Venäjän väestöön kohdistuvien operaatioiden tavoitteena on ylläpitää tuki sotatoimille. Ukrainan väestöön kohdistuvilla operaatioilla pyritään heikentämään luottamusta maan halukkuuteen torjua Venäjän hyökkäys. Yhdysvaltalaisiin ja eurooppalaisiin kohdistuva vaikuttaminen pyrkii heikentämään länsimaiden yhtenäisyyttä sekä torjumaan Venäjän sotarikoksia koskevaa kritiikkiä. Kolmansiin maihin kohdistuvilla operaatioilla Venäjä pyrkii ylläpitämään tai vahvistamaan näiltä valtioilta saamaansa tukea YK:ssa ja muissa kansainvälisissä järjestöissä (Microsoft, 2022b).

3.1 Media ja narratiivien levittäminen

Venäjän tiedustelupalveluilla, eli FSB:llä, GRU:lla ja SVR:llä, on Yhdysvaltojen viranomaisten arvion mukaan keskeinen rooli Venäjän disinformaation levittämisessä internetissä. FSB, GRU ja SVR pyörittävät nettisivujen verkostoa, joka pyritään tekemään houkuttelevaksi läntiselle yleisölle peittämällä sen venäläinen alkuperä (U.S. Department of the Treasury, 2021). Nämä sivut[3] ovat Recorded Future -tiedusteluyrityksen analyysin mukaan lähes varmasti ainakin toukokuusta 2022 lähtien toteuttaneet informaatiovaikuttamisoperaatioita nakertaakseen ja hajottakseen länsimaiden koalition tukea

[3] SouthFront -sivu on suoraan FSB:n ohjaama. NewsFront -sivu koordinoi narratiivejaan FSB:n kanssa. SVR ohjaa Strategic Culture Foundation -uutissivua ja epäilysten mukaan myös New Eastern Outlook -sivua. GRU puolestaan johtaa InfoRos -uutistoimistoa.

Ukrainalle. Sivujen levittämät informaatiovaikuttamisen narratiivit kuvaavat negatiivisesti ukrainalaisten pakolaisten vaikutuksia vastaanottajavaltioihin, syyttävät länsimaiden hallituksia energia- ja ruokakriisin aiheuttamisesta, lietsovat epäluottamusta länsimaisiin medioihin ja syyttävät Ukrainaa modernien fasististen liikkeiden luomisesta (Recorded Future, 2022).

Venäjän tiedustelupalvelut vaikuttavat myös sosiaalisessa mediassa. Ukrainan turvallisuuspalvelu SBU on jo vuonna 2021 osoittanut tiettyjen Telegram-kanavien[4] yhteyden GRU:hun (SBU, 2021). Kyseiset kanavat ovat täysmittaisen sodan syttymisen jälkeen julkaisseet sisältöä, jonka tarkoituksena on ollut heikentää ukrainalaisten luottamusta maan hallitukseen ja sen toimintaan Venäjän hyökkäyksen aikana. Sisällön tarkoituksena on ollut myös horjuttaa lännen tukea Ukrainalle (Wahlstrom ym., 2022).

FSB:n roolia informaatiovaikuttamisessa kuvaa myös Ukrainan turvallisuuspalvelun SBU:n sieppaama ja kesäkuussa 2022 julkaisema FSB:n viidennen direktoraatin asiakirja, jossa kuvataan Venäjän informaatiovaikuttamisen epäonnistumista Venäjän-Ukrainan sodan alkuvaiheessa. Asiakirjassa annetaan myös suosituksia mihin informaatiovaikuttamisen tulisi keskittyä tulevaisuudessa (SBU, 2022a).

3.2 Väärennökset ja deep fake -videot

Venäjän informaatiovaikuttamisen työkalupakkiin kuuluvat myös erilaiset väärennökset. Tämä toimintatapa on peräisin neuvostoajalta. Joissakin tapauksissa väärennetyt asiakirjat on toimitettu tiedotusvälineille väittäen, että ne on saatu hakkeroimalla. Vaikuttaa kuitenkin todennäköiseltä, että asiakirjat on joko tuotettu itse tai hankittu muita reittejä pitkin (Giles, 2016). Venäläinen vaikuttamiskampanja Secondary Infection käyttää väärennettyjä asiakirjoja, julkaisuja ja kuvakaappauksia venäjämielisten narratiivien levittämisessä. Kampanja on ollut aktiivinen jo ennen helmikuussa 2022 laajentunutta sotaa (Wahlstrom ym., 2022).

Venäjän ulkoministeriö julkaisi Twitterissä 9.3.2022 kuvia salaisesta asiakirjasta, jonka se väitti todistavan Ukrainan aikomuksen hyökätä Donbasiin maaliskuussa 2022 (MFA Russia, 2022). Faktatarkastajien mukaan asiakirja koski todellisuudessa Ukrainan sotaharjoitusta Lvivin alueella (Putterman, 2022).

Kuvia käytettiin hyväksi myös Kertšin sillan räjähdyksen uutisoinnissa. FSB syytti Ukrainan sotilastiedustelua räjähdyksestä, väittäen että sen aiheuttivat rekka-autoon sijoitetut räjähteet. Venäjän kontrolloima sivusto Ria Novosti julkaisi Telegram-kanavalla kameravalvontavideon väitetystä rekka-autosta, sekä väitetysti tullitarkastuksessa otetun röntgenkuvan, jossa näkyi auton sisältö. Julkaistujen kuvien ja videoiden rekka-autoissa oli kuitenkin eroja, mm. renkaiden määrässä ja vararengastelineessä. Kyse ei siten ollut samasta ajoneuvosta (Gigitashvili, 2022).

Ukrainan tiedustelupalvelu GUR kertoi lokakuun 2022 alussa, että Venäjän tiedustelupalvelut ovat *deep fake* -teknologian avulla yrittäneet esiintyä Ukrainan pääministeri Denys Šmyhalina etäkokouksessa Bayraktar Defense -yrityksen puheenjohtajan Haluk Bayraktarin kanssa. Tarkoituksena oli vahingoittaa Ukrainan ja Turkin yhteistyötä (Buziashvili, 2022). Vastaavaa on tapahtunut jo maaliskuun 2022 puolivälissä, kun

[4] Kyse on ainakin seuraavista kanavista: Legitimnyi, Resident, Cartel, Spletnitsa, Chornyi kvartal, Politicheskii rasklad, Netypichnoe Zaporozzhye, Trempel Kharkov, Odessa fraer, Dnepr live, Nikolaev live, Kherson live.

hakkerit murtautuivat Ukraine 24 -televisiokanavalle. Hakkeroinnin seurauksena televisiossa näytettiin *deep fake* -video, jolla presidentti Volodymyr Zelensky kehottaa ukrainalaisia laskemaan aseensa (Osadchuk, 2022).

3.3 Kyberhyökkäykset

Kuten aiemmin todettiin, Venäjän harjoittamaan informaatiovaikuttamiseen kuuluvat myös kyberoperaatiot. Venäjä on toiminut kyberympäristössä jo Itä-Ukrainan sodassa (Raitasalo, 2018). Ajoittain Venäjän kyberhyökkäykset ovat liittyneet sotilasoperaatioihin, joskus taas kyberhyökkäyksiä on käytetty kohteena olevan yhteiskunnan häiritsemiseen ja heikentämiseen. Venäjä on käyttänyt kybersuorituskykyjään myös uhkaillakseen hallituksia ja osoittaakseen tyytymättömyyttään tiettyihin tapahtumiin. Tämä todettiin mm. Volodymyr Zelenskyn puhuessa huhtikuussa 2022 Suomen eduskunnalle (Orenstein, 2022).

Venäjä toteutti vuonna 2022 useita kyberoperaatioita, kuten verkkohyökkäyksiä ja kybervakoiluoperaatioita. Venäjä pyrki haittaohjelmilla tuhoamaan järjestelmiä ja dataa. Se on myös toteuttanut verkkoihin murtautumisia ja kybervakoilua, joka on kohdistunut Ukrainan liittolaisiin, erityisesti Yhdysvaltoihin ja Puolaan. Myös Baltian maat, pohjoismaat ja Turkki ovat olleet kohteina (Microsoft, 2022b).

Venäjän tiedustelu- ja turvallisuuspalveluilla on ollut keskeinen rooli kybervaikuttamisessa. Microsoft julkaisi huhtikuussa 2022 raportin, jossa analysoitiin kaikki tiedossa olevat venäläisten verkkohyökkäykset Ukrainaa vastaan sodan ensimmäisinä kuukausina. Raportissa todetaan, että GRU, SVR ja FSB ovat suorittaneet tuhoisia kyberhyökkäyksiä ja vakoiluoperaatioita, joiden tavoitteena on ollut häiritä ja heikentää Ukrainan hallituksen ja asevoimien toimintaa, sekä horjuttaa ihmisten luottamusta instituutioihin (Microsoft, 2022a).

4 Ukraina

4.1 Ukrainan tiedustelupalvelun julkaisut

Ukrainan turvallisuuspalvelu SBU on julkaissut sodasta useita videoita ja artikkeleita nettisivuillaan. Julkaistun materiaalin tavoitteena on ollut vaikuttaa yleiseen mielipiteeseen ja nostaa Ukrainan puolustustahtoa. SBU:n informaatiovaikuttamiseen liittyvät julkaisut ovat sisältäneet usein videoita tai telekuuntelulla siepattuja venäläisten sotilaiden puheluita. Esimerkiksi julkaisu *”Professional Russian military can’t withstand pressure of AFU and write reports to terminate contracts”* (SBU, 2022b) kuvaa hyvin julkaisujen yhtenäistä kaavaa. Siinä tuodaan esille ensin narratiivi *”They have much better training than the newly mobilized ruscists, but even that is not enough to survive in Ukraine”*, perustellaan narratiivi nauhoitetulla materiaalilla, kehotetaan Venäjän sotilaita antautumaan ottamalla yhteyttä annettuun numeroon ja loppuun on lisätty kannustuslause Ukrainan voitolle.

Monet julkaistut videomateriaalit sisältävät myös lennokeilla kuvattua materiaalia. Esimerkki tällaisesta on The Guardian -lehdessä (Sabbagh, 2022b) julkaistu uutinen, johon on liitetty Ukrainan armeijan vuotama panssarintorjuntavideo. Video on 45 sekunnin mittainen editoitu kollaasi Venäjän panssaroitujen ajoneuvojen tuhoamisesta. Videon informaatiovaikuttamisen liittyvä tavoite selviää sen taustalle lisätystä nauhoitetusta puhelusta, jossa venäläinen viranomainen raportoi hyökkäyksestä. Toinen

esimerkki on SBU:n julkaisema video Venäjän jalkaväen taisteluajoneuvon tuhoamisesta (SBU, 2022c). Videon taustalle on lisätty sosiaalisen median alustan TikTokin kautta suosituksi nousseen musiikkigenren kappale, jolla mahdollisesti pyritään vetoamaan kohdeyleisöön ja lisäämään videon leviämistä. Näiden materiaalien tarkoituksena on kuvata sodan tilannetta ja erityisesti vahvistaa narratiivia heikosta hyökkääjästä. (Bronk ym., 2022).

4.2 Sosiaalinen media informaatiovaikuttamisen kanavana

Sosiaalisen median kanavat ovat olleet erityisen tärkeässä asemassa Ukrainan informaatiovaikuttamisen välineenä. Tilanteeseen on useita syitä. Julkaisuilla on sosiaalisen median alustojen suosion takia suuri ulottuvuus ja kohdeyleisö, videot voivat levitä näiden alustojen kautta hyvin nopeasti, ja julkaisujen levittäjinä voi olla useita toimijoita ja käyttäjiä (Johnson, 2022a). Esimerkiksi Ukrainan puolustusministeriön sosiaalinen media ja erityisesti Twitter-tili sisältävät paljon informaatiovaikuttamiseen pyrkiviä julkaisuja ja videoita. Muiden toimijoiden materiaalin levitys tapahtuu erityisesti TikTokissa, jossa lyhyet videot leviävät algoritmien myötä nopeasti laajalle käyttäjäkunnalle. Näissä videoissa narratiivia tai kontekstia ei usein taustoiteta, vaan videoissa vedotaan erityisesti tunteisiin ja pyritään lisäämään myötätuntoa Ukrainaa kohtaan (Rosenblatt ym., 2022).

Sosiaalisen median julkaisuilla voi nähdä olevan Venäjän-Ukrainan sodan osalta myös strateginen ja taktinen tarkoitus (Johnson, 2022b). Niiden kautta Ukraina on saanut tietoa joukkojen sijainneista ja dokumentaatiota tapahtumista. Sosiaalisen median avulla Ukraina on osoittanut taistelutahtoa ja näin välineistänyt sosiaalisen median palvelut informaatiovaikuttamisen alustoiksi.

Ukrainan harjoittama informaatiovaikuttaminen on monilta osin onnistunut. Se on lisännyt ukrainalaisten moraalia ja taistelutahtoa. Myös länsimaiden tuki Ukrainalle on ollut merkittävää. Ukrainan kuvien, videoiden ja uutisartikkeleiden avulla luoma narratiivi on lisännyt muiden maiden solidaarisuutta ja sympatiaa, samalla luoden pelkoa ja kaaosta sodan vastapuolelle (Johnson, 2022b). Yhdysvaltojen ja Euroopan Unionin antama tuki Ukrainalle on näkynyt esimerkiksi Venäjälle asetettujen sanktioiden ja Ukrainalle tarjotun taloudellisen tuen muodoissa (Feiner, 2022).

5 Yhdysvallat

Yhdysvaltojen *Global Engagement Centerin (GEC)* tehtäviä ovat muun muassa johtaa ja ohjata hallintoa tunnistamaan sekä torjumaan propagandaa ja disinformaatiota, joka kohdistuu Yhdysvaltoihin tai maan liittolaisiin (GEC, 2022). Disinformaation torjuntaan on käytössä kolme pääkeinoa. Ensimmäinen on osoittaa väitteet vääräksi ennen kuin ne saavat jalansijaa. Toinen ja ehkä intuitiivisin keino on vastaväite, jolla pyritään kumoamaan jo levinnyt disinformaatio. Kolmas on vastatoimi, jolla pyritään tuomaan esille disinformaation levittäjän motiiveja ja taustoja (GEC, 2020).

Useat Yhdysvaltojen ja Iso-Britannian toimet ovat olleet hyviä esimerkkejä *pre-bunking*-metodin käytöstä. Disinformaation etukäteen kumoaminen, *pre-bunking*, on valheiden, taktiikoiden tai lähteiden kumoamista ennen kuin ne vaikuttavat. Useat lähivuosina tehdyt tutkimukset kertovat tekniikan tehokkuudesta. Idea tekniikan takana on varoittaa ihmisiä heihin kohdistuvasta vaikuttamisesta, ja altistaa heitä esimerkeille disinformaatiosta (Nolan ym., 2021).

Yhdysvaltojen hallinto on toteuttanut uutta toimintatapaa informaatiosodankäynnissään Venäjää vastaan. Hallinto on pyrkinyt torjumaan Venäjän informaatio-operaatioita julkaisemalla tiedustelutietoja venäläisten aikeista Ukrainassa (Boot, 2022). Tiedustelutiedon jakamista julkisesti on tehty muun muassa kohdennetuilla tietojen vuotamisella valituille uutistoimistoille, sekä julkisilla lausunnoilla. Joissakin tapauksissa hallinnon käyttämät ulkopuoliset konsultit ja lainsäätäjät ovat luovuttaneet tietoja medialle (Toosi, 2022).

5.1 Ennakkovaroitus

Marraskuussa 2021 julkisuuteen tuli tietoja Yhdysvaltojen varoituksista Venäjän sotilasoperaation uhkasta Ukrainassa (Nardelli ym., 2021). Yhdysvaltojen ulkoministeri Antony Blinken kommentoi samaan aikaan Yhdysvaltojen seuraavan merkkejä Venäjän energiaaseen käyttämisestä politiikan välineenä Euroopassa. Energiakysymyksen lisäksi Blinken kommentoi Yhdysvaltojen olevan huolissaan Venäjän poikkeuksellisesta sotilaallisesta toiminnasta Ukrainan rajalla (Pamuk ym., 2021).

Joulukuun 3. päivänä vuonna 2021 Yhdysvallat luovutti medialle tiedustelutietoja, joiden mukaan Venäjä suunnittelee usean rintaman hyökkäystä Ukrainaan alkuvuodesta 2022. Venäjän operaation henkilöstövahvuudeksi arvioitiin jopa 175 000 sotilasta. Julkaistu aineisto sisälsi satelliittikuvia neljästä eri kohteesta, joihin Venäjä oli keskittänyt joukkoja. Arvioiden mukaan keskitetty voima vastasi noin 50 pataljoonan taisteluosastoa. (Harris ym., 2021).

5.2 False-flag-operaatioiden paljastaminen

Tammikuun 14. päivänä vuonna 2022 Valkoisen talon poliittinen neuvonantaja Jen Psaki kertoi lehdistötilaisuudessa Yhdysvaltojen tiedoista koskien venäläisiä operaattoreita, jotka valmistelivat *false-flag*-operaatiota Itä-Ukrainassa. Operaation tavoitteena arvioitiin olevan sabotaasi- ja informaatiovaikuttaminen, jolla lavastettaisiin Ukrainan hyökkäys venäläisiä joukkoja vastaan. Venäläiset vaikuttajat olivat jo ilmeisesti aloittaneet provokaatiot Ukrainan perinteisessä ja sosiaalisessa mediassa valmistellakseen Venäjän ”väliintuloa” sekä lisätäkseen kahtiajakoa ukrainalaisten keskuudessa. Venäjänkieliset valheelliset narratiivit sosiaalisessa mediassa, kuten lännen syyttäminen jännitteiden eskaloinnista, humanitaaristen ongelmien liioittelu Ukrainassa ja venäläisen isänmaallisuuden korostaminen, lisääntyivät kevään 2022 aikana noin 200 % marraskuuhun 2021 verrattuna (Psaki, 2022). Nimettömänä pysynyt yhdysvaltalainen viranomainen kertoi valtaosan *false-flag*-operaatioon liittyvästä tiedustelutiedosta olevan peräisin kaapatuista viesteistä ja henkilöseurannasta. (Garcia, 2022).

Helmikuun 2022 alussa Pentagonin lehdistösihteeri John Kirby kertoi lehdistötilaisuudessa tiedustelutiedosta, jonka mukaan yksi mahdollinen Venäjän *false-flag*-operaatio olisi lavastaa hyökkäys Venäjän maaperälle tai venäjää puhuvaa väestöä kohtaan. Tähän suunnitelmaan kuuluisi lisäksi väkivaltaisen propagandavideon kuvaaminen ja levittäminen. Videossa esitettäisiin ruumiita, surevia omaisia ja tuhoutuneita kohteita. Se syyttäisi Ukrainaa tai länsimaita hyökkäyksestä (Kirby, 2022a).

5.3 Putinin sisäpiiri

Tiedustelutietoa on julkaistu myös Kremlin sisäpiiristä. Helmikuussa 2022 nimettömänä pysyttelevien tiedustelulähteiden mukaan Yhdysvallat olisi kaapannut sanomia, joiden

mukaan osa Venäjän viranomaisista olisi ollut eri mieltä laajamittaisen hyökkäyksen järkevyydestä maan johdon kanssa. (Bertrand ym., 2022). Maaliskuun lopussa julkaistujen tietojen mukaan jännitteet kasvoivat Putinin ja puolustusministeriön välillä. Ulkoministeri Antony Blinkenin mukaan Putin olisi saanut vääriä tietoja neuvonantajiltaan (Barnes ym., 2022). Pentagonin lehdistösihteeri John Kirby kommentoi Yhdysvaltojen keräämien tietojen viittaavan siihen, että Venäjän puolustusministeriö ei olisi täysin informoinut Putinia maaliskuun aikana. Hän pitää mahdollisena, että Putinille ei kerrottu kaikkia tietoja operaatiosta, erityisesti Venäjän joukkojen vastoinkäymisistä Ukrainassa (Kirby, 2022b).

Lokakuussa lehdistölle vuodettiin tietoja, joiden mukaan Putinin sisäpiiriläinen olisi haastanut hänet Ukrainassa tehdyistä virheistä ja sodan huonosta johtamisesta (Buncombe, 2022). Tämän tyyppisten tietojen julkistamisella on voitu tavoitella Kremlin sisäpiirin horjuttamista (Crawford, 2022). Tietojen julkistaminen on voinut myös aiheuttaa epäilyä ja sekaannusta venäläisissä tiedustelupalveluissa, minkä seurauksena niiden operointikyky Ukrainassa on voinut pienentyä (Carvin, 2022).

6 Iso-Britannia

Iso-Britannian tiedusteluyhteisö on avautunut kuluneina vuosina. Ensimmäinen ulkomaantiedustelupalvelu MI6:n johtajan julkinen puhe nähtiin vuonna 2010. Tällainen viestiminen suoraan suurelle yleisölle on uusi toimintatapa tiedustelupalveluille. (Adam, 2022). Muutos voi osaltaan johtua Venäjän Krimin valtauksesta vuonna 2014 saaduista opeista. Jos tiedustelutietoja ei käytetä Venäjän narratiiviin vastaamiseen, menetetään etulyöntiasema (Sabbagh, 2022a).

Iso-Britanniassa Venäjän-Ukrainan sotaan liittyvästä informaatiosodankäynnistä vastaa hallinnon uusi informaatioyksikkö *Government Information Cell*, joka perustettiin helmikuussa 2022. Yksikkö toimii ulkoministeriön alaisuudessa, ja sen juuret ovat terrorismiin liittyvien informaatio-operaatioiden torjunnassa. Yksikössä työskentelee esimerkiksi venäjän kielen ja sosiaalisen median asiantuntijoita useista valtion organisaatioista. Heidän tehtävänään on kumota faktoilla Ukrainan sotaan liittyviä Venäjän valheellisia väitteitä (Government Communication Service, 2022).

6.1 Tiedustelun kasvava rooli julkisuudessa

Tammikuun 22. päivänä vuonna 2022 Iso-Britannian hallitus julkaisi tiedustelutietoja, joiden mukaan Venäjä suunnitteli nukkehallituksen asettamista Kiovaan. Viranomaisten mukaan heillä oli myös tietoja venäläisten tiedustelupalveluiden yhteyksistä entisiin ukrainalaisiin poliitikkoihin. Entisen presidentin Viktor Yanukovychin neljä liittolaista mainittiin henkilöiksi, joilla on yhteyksiä Venäjän tiedustelupalveluihin (Foreign, Commonwealth & Development Office, 2022).

Iso-Britannian puolustusministeriö aloitti tiedustelutiedon jakamisen sosiaalisessa mediassa helmikuussa 2022. Ministeriö jakaa edelleen tilannepäivityksiä Venäjän-Ukrainan sodasta. Julkaistavat tiedot ovat yleensä tiivistelmiä lähimenneisyyden tapahtumista ja arvioita tilanteen kehittymisestä. Välillä päivitykset sisältävät myös karttoja, jotka kuvaavat esimerkiksi Venäjän joukkojen hyökkäyssuuntia. Analyytikoiden ja viranomaisten mukaan läntisen tiedustelutiedon julkaisemien tukee Ukrainan

informaatiosodankäyntiä. Huomattavaa on myös se, että julkaistavat tiedot koskevat venäläisiä joukkoja. Tietoja Ukrainan joukkojen toiminnasta ei jaeta (Adam, 2022).

Iso-Britannian signaalitiedustelupalvelun johtaja Sir Jeremy Fleming piti puheen 31.3.2022, jossa hän puhui muun muassa Venäjän-Ukrainan sodasta. Fleming kävi läpi Venäjän asevoimien ongelmia, kuten sotilaiden heikkoa moraalia ja aseiden puutetta. Hän otti kantaa myös Putinin virhearvioihin ukrainalaisten vastarinnasta, sodan taloudellisista seurauksista ja asevoimiensa suorituskyvystä. Fleming avasi myös hieman uuden yksikön (engl. Government Information Cell) toimintaa. Hänen mukaansa yksi tehokkaista tavoista taistella disinformaatiota vastaan on kertoa totuus. Kasvavassa määrin monet näistä totuuksista tulevat tiedustelupalveluilta. Ukrainan sodan mukana tullut uusi ilmiö on salaisen tiedustelutiedon julkiseksi tekeminen nopealla aikataululla, jotta informaatiotilan hallinnassa voidaan olla askel edellä. Fleming viittaa muun muassa hyökkäysten ennakkovaroituksiin sekä *false-flag*-operaatioiden paljastamiseen. Hänen mukaansa tiedustelutiedon kerääminen on arvokasta vain, jos sitä käytetään, ja hän pitääkin tämänkaltaista kehitystä tervetulleena (GCHQ, 2022).

7 Johtopäätökset

Venäjän-Ukrainan sota on osoittanut, että Venäjän tiedusteluorganisaatioiden rooli informaatiovaikuttamisessa on keskeinen. Tiedusteluorganisaatiot luovat Venäjän narratiiveja tukevaa sisältöä teksti-, kuva- ja videomuodossa ja levittävät sitä peitesivustojen ja -kanavien kautta. Venäjä myös näennäisesti paljastaa ja julkaisee tiedustelutietoa informaatiovaikuttamisen tarkoituksessa. Toisin kuin länsimaiden ja Ukrainan hallintojen, Venäjän ei tarvitse miettiä, mitä tiedustelutietoa se julkaisee ja sanitoi. Maa ei pyri vaikuttamaan todenmukaisen informaation avulla, vaan se luo omien intressien mukaista tietoa. Venäjän tiedustelupalvelut pyrkivät informaatiovaikuttamisella heikentämään lännen tukea Ukrainalle ja horjuttamaan ukrainalaisten taistelumoraalia.

Ukrainan informaatiovaikuttamisen tavoitteena on puolestaan pyrkimys lisätä länsimaiden tukea ja nostaa ukrainalaisten taistelumoraalia. Ukrainan tiedustelupalveluilla on keskeinen rooli informaatiovaikuttamisessa käytettävän sisällön julkaisussa. Laajan yleisön saavuttamiseksi merkittävä osa sisällöstä pyritään levittämään myös erilaisilla sosiaalisen median alustoilla. Ukrainan informaatiovaikuttamisen narratiivin tarkoituksena on vedota tunteisiin muiden maiden tuen ja sympatian saamiseksi.

Yhdysvaltojen ja Iso-Britannian vastaus Venäjän informaatiosodankäyntiin näyttää toimivan. Venäjän informaatio-operaatioiden paljastaminen etukäteen on kaventanut Venäjän operaatiomahdollisuuksia. Tiedustelutietojen julkaiseminen on myös osaltaan voinut aiheuttaa Venäjän johdon ja tiedustelupalveluiden sisäisten jännitteiden kiristymistä. Ennakkovaroituksen antamisella on ollut läntisten valtioiden rintamaa yhdistävä vaikutus.

Mikäli pidemmällä aikavälillä informaatio-operaatioiden torjunnassa tiedustelutietojen avulla onnistutaan, toimiviksi havaittujen metodien käyttö jatkossa on todennäköistä. Onnistuessaan ennakkovaroitukset ja -paljastukset voivat myös parantaa länsimaisten tiedusteluorganisaatioiden mainetta ja julkisuuskuvaa.

Tiedustelutiedon julkaiseminen Venäjän-Ukrainan sodassa on ilmiönä uusi, joten siitä on niukasti tutkittua tietoa saatavilla. Monet saatavilla olevista lähteistä ovat uutisia. Lähteiden arvioimista on vaikeuttanut myös useiden organisaatioiden tyyli toimittaa

tietoja medialle nimettömänä. Tiedustelutiedon salainen luonne vaikeuttaa osaltaan tiedon arviointia, koska tietoihin viitataan usein puheissa, ilman konkreettisia todisteita.

Lähteet

Adam, K. (2022, April 22). How U.K. intelligence came to tweet the lowdown on the war in Ukraine. *The Washington Post.* https://www.washingtonpost.com/world/2022/04/22/how-uk-intelligence-came-tweet-lowdown-war-ukraine/

Akimenko, V., & Giles, K. (2020). Russia's cyber and information warfare. *Asia Policy*, 15(2), 67-75. https://www.proquest.com/scholarly-journals/russias-cyber-information-warfare/docview/2399206869/se-2

Balmas, M. (2014). When Fake News Becomes Real: Combined Exposure to Multiple News Sources and Political Attitudes of Inefficacy, Alienation, and Cynicism. *Communication research*, 41(3), 430-454. https://doi.org/10.1177/0093650212453600 (8.11.2022).

Barnes, J., Jakes, L., Ismay, J. (2022, March 30). U.S. intelligence suggests that Putin's advisers misinformed him on Ukraine. *New York Times.* https://www.nytimes.com/2022/03/30/world/europe/putin-advisers-ukraine.html

Bertrand , N., Sciutto, J., Bo Lillis, K. (2022, February). US intel indicates Russian officers have had doubts about full scale Ukraine invasion. *CNN*. https://edition.cnn.com/2022/02/07/politics/us-intel-russia-doubts-invasion-ukraine/

Bollfrass, A. K. (2017, December 19). How Does Intelligence Become Politicized? *Political Violence at a Glance.* https://politicalviolenceataglance.org/2017/12/19/how-does-intelligence-become-politicized/

Bronk, C., Collins, G., Wallach, D. (2022, September 6). Cyber and Information Warfare in Ukraine: What do We Know in Seven Months In? *Center for Energy Studies, Rice Unviersity's Baker Institute for Public Policy.* https://www.bakerinstitute.org/research/cyber-and-information-warfare-ukraine-what-do-we-know-seven-months

Boot, M. (2022, February 10). Why the U.S. Ramped Up Its Information War With Russia. *Council On Foreign Relations.* https://www.cfr.org/in-brief/why-us-ramped-its-information-war-russia

Buncombe, A. (2022, October 7). US intelligence tells Biden Putin was 'directly' confronted by angry Kremlin insider. *Independent.* https://www.independent.co.uk/news/world/americas/us- politics/biden-putin-kremlin-us-russia-ukraine-b2198111.html

Buziashvili, E. (2022, October 14). Russian deepfake attempt targeting Bayraktar drones CEO disrupted. In Russian War Report: Russia escalates war by targeting cities across Ukraine. *Digital Forensic Research Lab, Atlantic Council.* https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-russia-escalates-war-by-targeting-cities-across-ukraine/

Carvin, S. (2022, May 2). Deterrence, Disruption and Declassification: Intelligence in the

Ukraine Conflict. *Centre for International Governance Innovation.* https://www.cigionline.org/articles/deterrence-disruption-and-declassification-intelligence-in-the-ukraine-conflict/

Crawford, S. (2022, April 14). Preemptive, public US strikes winning intelligence war with Russia: ANALYSIS. *ABC News.* https://abcnews.go.com/Politics/preemptive-public-us-strikes-winning-intelligence-war-russia/story?id=84015518

Farwell, J. P. (2020). Information warfare: Forging communication strategies for twenty-first-century operational environments. Marine Corps University Press.

Feiner, L. (2022, March 1). Ukraine is winning the information war against Russia. *CNBC*. https://www.cnbc.com/2022/03/01/ukraine-is-winning-the-information-war-against-russia.html

Fogleman, R. R., Widnal, S. E. (1997). Cornerstones of Information Warfare. https://nsarchive.gwu.edu/sites/default/files/documents/4164297/United-States-Air-Force-Cornerstones-of.pdf

Foreign, Commonwealth & Development Office (2022, January 22). Kremlin plan to install pro-Russian leadership in Ukraine exposed. https://www.gov.uk/government/news/kremlin-plan-to-install-pro-russian-leadership-in-ukraine-exposed

Garcia, E. (2022, January 23). US intelligence says Russia planning false flag operation to justify Ukraine invasion. *Independent.* https://www.independent.co.uk/news/long_reads/world/russia-invasion-ukraine-us-false-flag-b1998878.html

GCHQ (2022, March 31). Director GCHQ's speech on global security amid war in Ukraine. https://www.gchq.gov.uk/speech/director-gchq-global-security-amid-russia-invasion-of-ukraine

GEC (2022). Core Mission & Vision. https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/

GEC (2020, February 11). Counter-Disinformation Dispatches #2. https://e.america.gov/t/ViewEmail/i/95383D12423453CD2540EF23F30FEDED/5069D0DCBA89C0A1EBAD456BEB5F1DD6

Gigitashvili, G. (2022, October 14). Russia blames Ukrainian military intelligence for Kerch bridge explosion. In Russian War Report Russia escalates war by targeting cities across Ukraine. *Digital Forensic Research Lab, Atlantic Council.* https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-russia-escalates-war-by-targeting-cities-across-ukraine/

Giles, K. (2016). Handbook of Russian Information Warfare. NATO Defence College, Rome.

Government Communication Service (2022, March 24). Responding to Russia's invasion. https://gcs.civilservice.gov.uk/news/responding-to-russias-invasion/

Harris, S., Sonne, P. (2021, December 3). Russia planning massive military offensive against Ukraine involving 175,000 troops, U.S. intelligence warns. *The Washington Post.* https://www.washingtonpost.com/national-security/russia-ukraine-

invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html

Hillebrand, C. (2012). The Role of News Media in Intelligence Oversight. *Intelligence and national security,* 27(5), 689-706. https://doi.org/10.1080/02684527.2012.708521

Johnson, D. (2022a, Feb 24). Ukraine Could Be the Most Documented War in Human History. *Slate*. https://slate.com/technology/2022/02/ukraine-russia-livestream-google-maps.html

Johnson, D. (2022b, March 27). The real reason Ukraine's information war is so successful. *Task & Purpose.* https://taskandpurpose.com/news/ukraine-information-war/

Kagubare, I. (2022, May 3). State-backed hackers ramp up cyber operations in Eastern Europe: Google. *The Hill.* https://thehill.com/policy/international/3475914-state-backed-hackers-ramp-up-cyber-operations-in-eastern-europe-google/

Kari, M. J. (2022, April 21). Taistelu informaatiosta Ukrainan sodassa. *Suomen Sotatieteen Seuran Studia Miltaria.* https://www.youtube.com/watch?v=fRUCYA1PxBo

Kirby, J. (2022a, February 3). Pentagon Press Secretary John F. Kirby Holds a Press Briefing. *U.S. Department of Defence.* https://www.defense.gov/News/Transcripts/Transcript/Article/2922998/pentagon-press-secretary-john-f-kirby-holds-a-press-briefing/

Kirby, J. (2022b, March 30). Pentagon Press Secretary John F. Kirby Holds a Press Briefing. *U.S. Department of Defence.* https://www.defense.gov/News/Transcripts/Transcript/Article/2983648/pentagon-press-secretary-john-f-kirby-holds-a-press-briefing-march-30-2022/

MFA Russia (2022, March 9). Twitter https://archive.ph/QMaea

Microsoft (2022a, April 27). Special Report: Ukraine, An overview of Russia's cyberattack activity in Ukraine. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

Microsoft (2022b, June 22). Defending Ukraine: Early Lessons from the Cyber War https://wwps.microsoft.com/content/defending-ukraine-early-lessons-from-the-cyber-war

Napper, J. (2020). Fake News or Information Warfare? Signal, 74(11), 56.

Nardelli, A., Jacobs, J., Wadhams, N. (2021, November 12). U.S. Warns Europe That Russia May Be Planning Ukraine Invasion. *Bloomberg*. https://www.bloomberg.com/news/articles/2021-11-11/u-s-warns-europe-that-russian-troops-may-plan-ukraine-invasion

Nolan S., Kimball M. (2021, August 27). What Is Prebunking? *Psychology Today.* https://www.psychologytoday.com/us/blog/misinformation-desk/202108/what-is-prebunking

OECD (2022, November 3). Disinformation and Russia's war of aggression against Ukraine: Threats and governance responses. https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-

ukraine-37186bde/

Orenstein, M. (2022, June 7). Russia's Use of Cyberattacks: Lesson from the Second Ukraine War. *Foreign Policy Research Institute.* https://www.fpri.org/article/2022/06/russias-use-of-cyberattacks-lessons-from-the-second-ukraine-war/

Osadchuk, R. (2022, March 16). Hacked new program and deepfake video spread false Zelenskyy claims. In Russian War Report: Hacked new program and deepfake video spread false Zelenskyy claims. *Digital Forensic Research Lab, Atlantic Council.* https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-hacked-news-program-and-deepfake-video-spread-false-zelenskyy-claims/

Pamuk, H., Lewis, S. (2021, November 10). Blinken meets Ukraine official, warns Russia on natgas supplies. *Reuters.* https://www.reuters.com/world/europe/blinken-meets-ukraine-official-warns-russia-natgas-supplies-2021-11-10/

Pelletier, J. (2022, March 1). Intelligence, information warfare, cyber warfare, electronic warfare – what they are and how Russia is using them in Ukraine. *The Conversation.* https://theconversation.com/intelligence-information-warfare-cyber-warfare-electronic-warfare-what-they-are-and-how-russia-is-using-them-in-ukraine-177899

Putterman, S. (2022, March 9). No, this document doesn't show classified Ukrainian military orders to attack the Donbas region. *Politifact.* https://www.politifact.com/factchecks/2022/mar/14/tweets/no-document-doesnt-show-secret-ukrainian-military-/

Psaki, J. (2022, January 14). Press Briefing by Press Secretary Jen Psaki and FEMA Administrator Deanne Criswell. *The White House.* https://www.whitehouse.gov/briefing-room/press-briefings/2022/01/14/press-briefing-by-press-secretary-jen-psaki-and-fema-administrator-deanne-criswell-january-14-2022/

Pynnöniemi, K. (2019). Information-psychological warfare in Russian security strategy. In Kanetm R, (ed.), *Routledge Handbook of Russian Security Policy*. Routledge - Taylor & Francis Group, London and New York, pp. 214-226.

Raitasalo, J. (2018). Hybridisota ja hybridiuhat – paljon vanhaa…onko mitään uutta? Tiede Ja Ase, 76.

Recorded Future (2022, July 7). Insikt Group, Russian Information Operations Aim to Divide the Western Coalition on Ukraine. Cyber Threat Analysis, Russia. https://go.recordedfuture.com/hubfs/reports/ta-2022-0707.pdf

Rosenblatt, K., Tenbarge, K. (2022, March 4). Ukraine fights back on TikTok, where war is fought with memes and misinformation. *NBC News.* https://www.nbcnews.com/tech/tech-news/tiktok-ukraine-war-misinformation-propaganda-rcna18146

Sabbagh, D. (2022a, February 18). Ukraine crisis brings British intelligence out of the shadows. *The Guardian.* https://www.theguardian.com/world/2022/feb/18/ukraine-crisis-bring-british-intelligence-out-of-the-shadow-warning-russian-invasion-information-war-with-kremlin

Sabbagh, D. (2022b, March 10). Drone footage shows Ukrainian ambush on Russian

tanks. *The Guardian.* https://www.theguardian.com/world/2022/mar/10/drone-footage-russia-tanks-ambushed-ukraine-forces-kyiv-war

SBU (2021, February 1). SBU exposes Russian agent network. https://ssu.gov.ua/en/novyny/sbu-vykryla-ahenturnu-merezhu-spetssluzhb-rf-yaka-destabilizuvala-sytuatsiiu-v-ukraini-cherez-telegramkanaly

SBU (2022a, June 5). SBU otrymala dostup do propahandystskykh metodychok rosiiskykh spetssluzhb pro "pravylne vysvitlennia spetsoperatsii" v Ukraini (video) https://ssu.gov.ua/novyny/sbu-otrymala-dostup-do-propahandystskykh-metodychok-rosiiskykh-spetssluzhb-pro-pravylne-vysvitlennia-spetsoperatsii-v-ukraini-video

SBU (2022b, October 30). Professional russian military can't withstand pressure of AFU and write reports to terminate contracts. https://ssu.gov.ua/en/novyny/profesiini-viiskovi-rf-ne-vytrymuiut-natysku-zsu-i-masovo-pyshut-raporty-na-rozirvannia-kontraktiv

SBU (2022c, October 24). SSU Counterintelligence destroys enemy infantry fighting vehicle with 'three-point shot' in hatch (video). https://ssu.gov.ua/en/novyny/spivrobitnyky-viiskovoi-kontrrozvidky-sbu-trokhochkovym-postrilom-u-liuk-znyshchyly-vorozhu-bmp-u-donetskii-oblasti-video

Shpiro, S. (2001). The Media Strategies of Intelligence Services, *International Journal of Intelligence and CounterIntelligence*, 14:4, 485-502, DOI: 10.1080/08850600152617128

Teirila, O. (2016). Intelligence and Media: Multidimensional Effects of Publicity. *American Intelligence Journal*, 33(2), 137–143.

Toosi, N. (2022, August 2). Spy world wary as Biden team keeps leaking Russia intel. *Politico.* https://www.politico.com/news/2022/02/08/spy-world-biden-leaking-russia-intel-00006956

U.S. Department of the Treasury (2021, April 15). Press Release: Treasury Escalates Sanctions Against Russian Government's Attempt to Influence U.S. Elections. https://home.treasury.gov/news/press-releases/jy0126

VNK (2019, April 5). Informaatiovaikuttamiseen vastaaminen: Opas viestijöille. *Valtioneuvoston kanslia.* https://julkaisut.valtioneuvosto.fi/handle/10024/161512

Wahlstrom, A., Revelli, A., Riddel, A., Mainor, D., Serabian A. (2022, May 19). The IO Offensive: Information Operation Surrounding the Russian Invasion of Ukraine. *Mandiant.* https://www.mandiant.com/resources/blog/information-operations-surrounding-ukraine

SUOJELUPOLIISIN VUOSIKIRJAT JA NIISSÄ TAPAHTUNEET UHKAKUVIEN MUUTOKSET 2015-2021

Johanna Kangas, Maare Paloheimo, Ristomatti Väänänen

1 Johdanto

1.1 Lähtökohdat

> Uudessa normaalissa – tämän päivän turvallisuusympäristössä – uhka voi tulla odottamattomalta suunnalta ja muodossa, johon ei ole aiemmin totuttu. (Suojelupoliisin vuosikirja 2016, 4).

Raportin tarkoituksena on selvittää Suomen sisäisestä turvallisuudesta vastaavan viranomaisen, Suojelupoliisin (Supo), tuottamien julkisten vuosikirjojen perusteella, millaisia uhkakuvia Suomeen on kohdistunut vuosina 2015–2021. Raportissa ei tarkastella Suojelupoliisin toimintaa tai organisaatiota vaan sitä, millaisia painotusmuutoksia uhkakuvissa on tapahtunut tarkastelujaksolla Suojelupoliisin näkökulmasta. Päälähteenä käytettävät Suojelupoliisin vuosikirjat kuvaavat tarkasteluvuosien turvallisuusympäristöä, sen keskeisiä muutoksia sekä kertovat yleisellä tasolla Suojelupoliisin toiminnasta.

Vuosikirjoja on julkaistu nykymuotoisina vuodesta 2015 alkaen, ja tämän raportin tuorein kattaa vuoden 2021 tapahtumat. Aikavälillä 2015–2021 on mahdollista tarkastella systemaattisemmin erilaisia uhkailmiöitä ja havainnoida niiden kehityslinjoja. Tarkastelun aloittamista vuodesta 2015 tukee se, että vuosikirjan julkaisemisen myötä myös Suojelupoliisin viestinnällinen tyyli muuttui. Ennen tätä Suojelupoliisi julkaisi tiiviitä, asiakeskeisiä vuosikertomuksia aina vuodesta 1994 lähtien (Supo 2014; Simola (toim.) 2009).

Raporttia tehtäessä vuosien 2016–2021 vuosikirjat ovat olleet saatavilla Suojelupoliisin verkkosivuilla (supo.fi). Vuoden 2015 vuosikirja, joka oli poistettu verkkosivuilta, sekä vuosien 2010–2014 vuosikertomukset on pyydetty Suojelupoliisin viestinnästä. Vuosikirjat ja -kertomukset ovat julkista materiaalia ja varhaisimmat niistä on julkaistu painettuina. Vuosikertomuksia 2010–2014 käytetään taustoittavina lähteinä, minkä lisäksi raportissa viitataan julkisesti saatavilla oleviin Kansallisen turvallisuuden katsauksiin vuosilta 2018–2022. Katsauksissa tarkastellaan lyhyesti Suojelupoliisin toimialaan kuuluvia ilmiöitä ja arvioidaan kehityslinjoja, joten ne tukevat hyvin tässä esitettävää analyysia. Tutkimuskirjallisuus ja erilaiset muut aineistot täydentävät kuvaa.

Raportti keskittyy kolmeen tutkimuskysymykseen, jotka ovat:

1) Millaisia uhkia tai uhkakuvia Suojelupoliisin vuosikirjoista voidaan tunnistaa?
2) Miten uhkakuvat kuvataan?
3) Muuttuvatko esitetyt uhkakuvat tai voidaanko niissä tunnistaa painotusmuutoksia?

Näihin kysymyksiin vastataan luvuissa 2–6. Tiettyjen uhkakuvien, kuten terrorismin ja radikalisoitumisen uhkien, yksityiskohtaisempi käsittely on perusteltua Suomen turvallisuustilanteessa ja globaalissa ympäristössä tapahtuneen nopean muutoksen takia.

1.2 Suojelupoliisin vuosikirjat ja niissä esiintyvien uhkien tarkastelu

Tässä raportissa uhkakuva viittaa uhkaan tai epävarmuustekijään, jonka toteutuminen katkaisee rauhanomaisen, vakaan (yhteiskunnallisen) kehityksen tai aiheuttaa muutoin merkittäviä häiriöitä. Pahimmillaan uhka haastaa valtion ja kansan olemassaolon. Tässä yhteydessä keskeistä on myös se, että uhka kohdistuu etenkin kansalliseen turvallisuuteen, suomalaiseen demokraattiseen järjestelmään tai yleensä yhteiskunnan normaaliin toimintaan ja järjestykseen. Uhat ja uhkakuvat muuttuvat ajan myötä, mutta osa turvallisuuden vaikuttavista tekijöistä on pysyviä (Limnéll & Iloniemi 2018; Laitinen & Huhtinen 2021). Myös tarkasteltujen vuosikirjojen perusteella voidaan todeta osan uhkailmiöistä olevan pysyviä ja osan taas muodoltaan muuttuvia: kuvaava esimerkki on hybridivaikuttaminen, joka voi ilmetä erilaisina vaikuttamisyrityksinä tai -kampanjoina, joilla vaikuttajataho pyrkii saavuttamaan omia tavoitteitaan (ks. luku 3).

Vuosikirjoissa esitettyjä uhkakuvia ja niiden muutosta tarkasteltaessa on huomioitava, että tarkasteluvuosien aikana Suojelupoliisin organisaatio, strategia ja toimivaltuudet ovat muuttuneet monin tavoin. Vuosikirjoissakin mainittu merkittävä muutos on ollut uusien tiedustelulakien voimaantulo 1.6.2019. Laissa säädetään muun muassa Suojelupoliisin tiedonhankinnasta ja tiedon hyödyntämisestä kansallisen turvallisuuden suojaamiseksi. Laissa säädetyt siviilitiedustelumenetelmät ovat vain Suojelupoliisin käytössä, ja tämän myötä tiedonhankinnan painopiste on siirtynyt aikaisempaa varhaisempaan vaiheeseen – kykyyn havaita ja reagoida uhkia aikaisemmin (Sisäministeriö 2019). Suojelupoliisi katsoo myös uuden lainsäädännön antavan tukevan pohjan tehtävien suorittamiselle (Supo 2019). Nämä seikat heijastuvat vuosikirjoihin: niissä esitellään organisaation tehtäviä, työmenetelmiä ja lainsäädäntömuutoksia, sikäli kun ne ovat vaikuttaneet organisaation toimintaan. Nämä teemat rajataan kuitenkin tämän raportin ulkopuolelle.

Vuosikirjat ovat muuttuneet 2020-luvulle tultaessa visuaalisemmiksi kokonaisuuksiksi, ja ne sisältävät asiantuntijahaastatteluja. Niiden sisältöä analysoitaessa on huomioitava, että ne ovat osa organisaation strategista viestintää ja suunnattu erilaisille asiakas- ja sidosryhmille sekä laajemmallekin yleisölle. Tarkastelujaksoon osui kaksi juhlavuotta, Suomi 100 vuotta ja Suojelupoliisi 70 vuotta, jolloin vuosikirjojen aihepiirit olivat tavanomaista laajempia (Supo 2016; 2018b).

Raporttiin on koottu keskeisimmät vuosikirjoissa esitetyt uhkakuvat laadullisen analyysin keinoin (sisällönanalyysi, tutkimusteemoihin liittyvät hakusanat). Tarkastelun kohteena olleiden vuosikirjojen perusteella voidaan todeta kansalliseen turvallisuuteen kohdistuneen monimuotoisia ja osin uusia uhkia. Tässä raportissa on tunnistettu seuraavat uhkakuvat tai uhat: 1) ulkovaltojen valtiollinen vaikuttaminen, 2) hybridi- ja kyberuhat sekä informaatiovaikuttaminen, 3) terrorismi, radikalisoituminen ja ääriliikkeiden muodostama uhka, 4) pakolaisvakoilu ja 5) kriittiseen infrastruktuuriin sekä yritys-, tiede- ja tutkimustoimintaan kohdistuvat uhat.

Nämä uhkailmiöt on valittu lähemmän tarkastelun kohteiksi vuosikirjoista havaittujen kuvausten, ilmaisujen ja käytettyjen käsitteiden pohjalta. Joidenkin ilmiöiden osalta aineistosta esiin nousevat uhat on pyritty sitomaan laajempaan kontekstiin –

kuten esimerkiksi huoltovarmuuden ylläpitoon liittyvät uhat, jotka tulevat usein esille kriittisen infrastruktuuriin kohdistuvien uhkien yhteydessä. Samalla tavoin hybridi- ja kyberuhkia sekä informaatiovaikuttamista tarkastellaan kokonaisuutena, sillä ne limittyvät vuosikirjoissa toisiinsa. Vuosien 2010–2014 vuosikertomuksia käytetään taustoittamaan tärkeimpien uhkakuvien kehitystä ja muutosta, arvioimatta kuitenkaan yksityiskohtaisesti uhan kehittymistä tuolta ajalta nykyhetkeen.

2 Ulkovaltojen valtiollinen vaikuttaminen

Maantieteellisen sijaintinsa takia Suomeen on kohdistunut aktiivista ja pysyväisluonteista ulkovaltioiden tiedustelutoimintaa. EU-jäsenyyden myötä Suomesta tuli väylä saada tietoa läntisen maailman toimintatavoista. Naapurimaa Venäjän tiedustelua Suomessa on edesauttanut maantieteellinen läheisyys sekä taloudellinen ja kulttuurinen yhteistyö. Suomen Venäjä-suhteeseen ovat lyöneet oman leimansa sotilaalliset uhkakuvat, epävarmuus Venäjän kehityksen suunnasta ja sen vaikutuksesta Suomen turvallisuusympäristöön (Haukkala 2020). Venäjän vaikutusta Suomessa ja lähialueilla käsitellään Suojelupoliisin vuosikirjoissa ja niiden rinnalle nousee myös Kiinan valtiollisen vaikuttamisen voimistuminen 2020-luvulle tultaessa. (Supo 2018b)

Vuosikirjoissa ulkovaltojen kiinnostuksen Suomea kohtaan mainitaan olleen pitkäaikaista. Tämän seurauksena Suomi on toiminut asemapaikkana verrattain suurelle määrälle ulkovaltojen tiedustelupalveluiden henkilöstöä (esim. Supo 2016; 2021b). Ulkovaltojen tiedustelutoiminta on ollut aktiivista ja monimuotoista koko tarkastelujaksolla. Tiedustelun intensiivisyys on luonnollisesti vaihdellut ja tiettyinä aikoina ulkomaisten tiedustelupalveluiden toiminta on ollut aggressiivisempaa (Supo 2015; 2020). Ulkovaltojen tiedustelupalveluilla on käytössään laaja arsenaali erilaisia vaikuttamistapoja sekä erilaisia menetelmiä, joilla voidaan esimerkiksi kontaktoida potentiaalisia kohdehenkilöitä (Supo 2016. Ks. myös Althoff 2016).

Koronapandemian aikana voimassa olleet poikkeukselliset matkustus- ja kokoontumisrajoitukset hankaloittivat ulkovaltojen henkilötiedustelua Suomessa. Lyhyen hiljaisen jakson jälkeen valtiot ryhtyivät kuitenkin panostamaan aiempaa aktiivisemmin kybervakoiluun. Muutokseen vaikutti muun muassa laajasti yleistynyt etätyöskentely (Supo 2020b, ks. myös alaluku 3.2). Vuosikirjojen mukaan ulkovaltojen vakoilu saattaa ulottua hyvinkin korkealle yhteiskunnassa: tiedustelupalveluita on kiinnostanut erityisesti henkilöt, jotka pääsevät käsiksi ei-julkiseen tietoon tai joilla on mahdollisuuksia vaikuttaa päätöksentekoprosesseihin (Supo 2021b). Henkilötiedustelun katsotaan olevan pitkäjänteistä toimintaa, mistä kertoo ulkovaltojen tiedustelun pyrkimys löytää kohteiksi nuoria potentiaalisia yhteiskunnallisia vaikuttajia. Lisäksi ulkovallat voivat pyrkiä vaikuttamaan kansalaismielipiteeseen (Supo 2021b, ks. myös alaluku 3.1). Pandemian myötä muuttunut tilanne ei kuitenkaan vähentänyt tai poistanut perinteisen henkilöiden kautta tapahtuvan vakoilun uhkaa Suomessa (Supo 2020b). Suomeen kohdistuvan tiedustelun uhan on arvioitu voimistuvan kireän turvallisuuspoliittisen tilanteen takia (Supo 2021b).

Valtiolliseen vakoilutoimintaan heijastuvat luonnollisesti myös kansainvälinen poliittinen tilanne ja jännitteet. Vakoiluyrityksiä on esimerkiksi kohdentunut suomalaisen ulko- ja turvallisuuspoliittisen päätöksenteon valmisteluun viime vuosien aikana. Valtioiden välisten suhteiden kiristymisen heikentäessä mahdollisuuksia hankkia tietoa laillisia kanavia pitkin, lisääntyy myös valtiollinen vakoilutoiminta tiedon tarpeen kasvaessa

(Supo 2019). Tavanomaisen diplomaattisen toiminnan estyessä ja valtioiden välisen vastakkainasettelun lisääntyessä salaisen tiedonhankinnan kysyntä ja merkitys kasvaa. Valtiollisella tiedustelutoiminnalla ja vakoilulla tavoitellaankin sellaista informaatiota, jota kyseisellä hetkellä ei olisi muulla tavoin mahdollista saada. Viime vuosien globaali demokraattisten oikeusvaltioiden ja autoritääristen valtioiden lisääntynyt vastakkainasettelu on edelleen kasvattanut jälkimmäisten kiinnostusta hankkia vakoilemalla salaista tietoa vieraista valtioista. Etenkin päätöksentekoon ja edistykselliseen teknologiaan liittyvän tiedon hankkiminen oikeudetta on nähty uhkana. (Supo 2021b)

Uusimpien vuosikirjojen perusteella Suomen kansallista turvallisuutta uhkaavaa vakoilua kohdistuu Suomeen enimmäkseen Venäjän ja Kiinan taholta (Supo 2020b; 2021b). Kyseisten valtioiden kiinnostus on kohdistunut erityisesti Suomen poliittisiin linjauksiin ja toimintaan arktisella alueella. Venäjän ja Kiinan kiinnostusta arktista aluetta kohtaan motivoi pyrkimykset oman vaikutusvallan vahvistamiseen alueella sekä laajemmin globaalilla tasolla (Supo 2019, ks. luku 6). Poliittisten vastakkainasettelujen eskaloituminen ja useat nykyiset epävarmuustekijät lisäävät huolta uhkien voimistumisesta. Venäjän aktiivinen tiedustelu- ja vaikuttamistoiminta, kiinnostus Suomen Nato-suhdetta kohtaan sekä teknologian ja osaamispääoman vakoilu ovat uhkina läsnä myös vuoden 2022 kansallisen turvallisuuden katsauksessa. (Supo 2022a)

3 Ennalta-arvaamatonta ja monimuotoista vaikuttamista

3.1 Hybridivaikuttaminen

Vuoden 2015 vuosikirjassa todettiin Suomen turvallisuusympäristön muuttuneen vaikeammin ennustettavaksi ja monimutkaisemmaksi (Supo 2015). Kiristynyt turvallisuuspoliittinen tilanne ja suurvaltojen jännittyneet suhteet tulevat todennäköisesti voimistamaan myös Suomeen kohdistuvaa tiedustelua (Supo 2021). Turvallisuusympäristön nopean muutoksen myötä voidaan nykytilaa kutsua uudeksi normaaliksi, missä uhka voi ilmetä ennennäkemättömällä tavalla ja muodossa (Supo 2016). Esimerkiksi Jarno Limnéll ja Jukka Iloniemi kirjoittavat kirjassaan Uhkakuvat (2018), että uhat, joiden on arvioitu vaarantavan turvallisuuttamme, vaihtuvat ajan myötä. Kirjassa määritellään hybridivaikuttamisen keinojen noudattavan vanhojen sodankäyntitaitojen periaatteita: “Toiminta tulee olla yllätyksellistä ja harhauttavaa, oma toiminta ja päämäärät on salattava sekä aloite tulee pitää omissa käsissä” (Limnéll & Iloniemi 2018, 107). Hybridivaikuttamisessa ei ole heidän mukaansa kyse dramaattisesta hyökkäyksestä vaan ns. sodan julistamisen kynnyksen alapuolella toteutettavista pienistä ja jatkuvista vaikutuskeinoista, jolla sodan ja rauhan välistä rajaa pyritään tietoisesti hämärtämään. Edellä esitetyt kuvaukset hybridivaikuttamisesta näkyvät esimerkiksi Suojelupoliisin vuoden 2018 vuosikirjassa, jossa hybridivaikuttamisen todetaan olevan erityisesti suurvaltojen harjoittamaa, laajan keinovalikoiman toimintaa omien etujen edistämiseksi. Toiminnan tavoitteena on kohdevaltion vahingoittaminen haavoittuvuuksia hyödyntämällä ja salaamalla todellinen vaikuttamistaho (Supo 2018b).

Vuosina 2015–2021 hybridivaikuttaminen on ollut jatkuvasti näkyvä ilmiö. Sen voimakkuus ja monimuotoistuminen tekee siitä aiempaa suuremman turvallisuusuhan (Supo 2018b). Vuosikirjojen kuvauksista voidaan ymmärtää hybridivaikuttamisen olevan pysyvä ja hiljalleen kasvanut uhka. Suomeen kohdistuviksi mahdollisiksi vaikuttamiskeinoiksi on katsottu esimerkiksi informaatiokampanjat, poliittinen painostus,

rajavakauden horjuttaminen, taloudellisen vaikutusvallan kasvattaminen ja talouselämän kielteisten ilmiöiden hyväksikäyttäminen (Supo 2018b, ks. alaluku 3.3).

Hybridivaikuttamisen uhan voidaankin näin ollen todeta ulottuvan hyvin eri tasoille yhteiskunnassamme, niin kansalaisiin kuin päättäjiin. Vuosikirjoista voidaan päätellä myös, että ulkovaltojen yhtenä hybridivaikuttamisen tavoitteena on vaikuttaa päättäjien tilannekuvan muodostamiseen. Ulkoministeriön poliittisen osaston päällikkö Mikko Kinnunen toteaa hybridiuhkien torjunnassa korostuvan eri viranomaisten välinen tiedonjako yhteisen ja oikean tilannekuvan muodostamiseksi (Supo 2020). Vastaavasti Limnéll ja Iloniemi (2018) painottavat yhteistyön merkitystä muuttuvassa turvallisuusympäristössä: keskeisenä nähdään turvallisuustoimijoiden perinteisten jakolinjojen ylittäminen ja uhkien yhteinen ymmärrys. Edellä mainitun lisäksi yhteistyön merkitystä ei voi olla korostamatta liikaa nyt ja tulevaisuudessa, sillä oikea-aikainen ja luotettava tieto tukee myös valtiojohdon päätöksentekoa monimutkaisissa tilanteissa. (Supo 2015).

Suojelupoliisi pitää Venäjän hybridivaikuttamista ja laitonta tiedustelua suurimpina kansallisen turvallisuuden uhkina Suomessa (Supo 2021b). Vaikka Suomeen kohdistuvissa vaikuttamistoimissa ei ole odotettavissa muutoksia (Supo 2021a), Limnéll ja Iloniemi (2018) ovat pitäneet positiivisena asiana sitä, että suhteessa moneen muuhun länsimaahan Suomi on hieman immuunimpi hybridivaikuttamiselle. Heidän mukaansa tähän vaikuttaa Suomen kansallinen yhtenäisyys, koulutustaso, viranomaisyhteistyö ja poliittinen vakaus. Länsimaiden panostus hybridivaikuttamisen torjuntaan on todettu vähentävän tätä uhkaa (Supo 2020a).

3.2 Kyberuhat

Suojelupoliisin vuosikirjoissa kyberuhat näyttäytyvät monitahoisena uhkakokonaisuutena ja koko tarkastelujaksoa leimaavatkin lukuisat kyberhyökkäykset tai niiden uhka. Yksi kyberuhkien muoto on kybervakoilu, jota kuvataan tietoverkoissa tapahtuvaksi tiedonhankintaoperaatioksi (Supo 2019). Toimintaa eivät rajoita fyysisen maailman rajat, jolloin myös kiinnijääminen on epätodennäköisempää (Limnéll & Iloniemi 2018). Suoraan Suomeen kohdistuvan hyökkäyksen lisäksi kybervakoilija voi naamioida toimintansa siten, että se näyttää Suomen tai suomalaisesta verkosta toteutetulta operaatiolta johonkin toiseen valtioon (Supo 2016). Luottamukselliseksi tarkoitettua tietoa voidaan hankkia esimerkiksi hyödyntämällä tietojärjestelmien teknisiä haavoittuvuuksia tai erilaisin painostustoimin, kuten pyrkimällä vaikuttamaan suoraan laite- ja ohjelmistotoimittajiin (Supo 2019). Vuosikirjojen perusteella voidaan todeta, että huoltovarmuuskriittisiin kohteisiin kohdistuva tiedustelu tapahtuu erityisesti kybermaailmassa. Vakoilu voi kohdistua näiden kohteiden lisäksi myös tavallisiin yrityksiin ja merkityksellistä onkin se, millainen jälleenmyyntiarvo vakoiltavalla kohteella on. Erityisesti tuotekehitystä tekevät yritykset ovatkin joutuneet kybervakoilun kohteeksi. (Elinkeinoelämän keskusliitto 2018; Supo 2016).

Toisena hyökkäysesimerkkinä vuosikirjoissa on esitetty automatisoidut palvelunestohyökkäykset, joiden tarkoituksena on aiheuttaa epäluottamusta kyberympäristön toimintaan. Automatisoinnin ansiosta nämä hyökkäysmuodot ovat helppoja toteuttaa ja mahdolliseksi hyökkäyksen kohteeksi on katsottu etenkin kriittinen infrastruktuuri. (Supo 2022a, ks. myös luku 6)

Useat tekijät voivat voimistaa yllä kuvattuja uhkakuvia: hyvä esimerkki tästä on talouselämässä yleinen tapa ulkoistaa tiedon hallinnointia alihankkijoille, jolloin

tiedonhallintarakenteita voi olla vaikeampaa kontrolloida. Tästä syystä hankintojen riskienhallintaprosessi korostuukin kybervakoilun torjunnassa. Toisaalta tiedustelulainsäädännön muutos vuonna 2019 on laajentanut mahdollisuuksia kyberuhkien torjuntaan. (Supo 2017; 2019)

Koronapandemian myötä kybervakoilussa tapahtui merkittävä muutos, sillä vakoilun painopiste siirtyi aiempaa enemmän verkkoympäristöön matkustus- ja liikkumisrajoitusten takia sekä työskentelyn siirtyessä pääosin etäyhteyksien varaan. Tämä aiheutti myös poliittisten päätösten valmistelun siirtymisen verkkoon ja erityisesti sähköposteihin. Tämän seurauksena sähköpostiliikenteen vakoilun uhka kohosi. (Supo 2020b, ks. myös luku 2)

3.3 Informaatiovaikuttaminen

Informaatiovaikuttaminen voidaan määritellä suunnitelmallisiksi viestinnän ja vaikuttamisen keinoiksi, joiden päämääränä on informaatiota muokkaamalla aikaansaada muutoksia kohteen informaatio- ja mielipideympäristössä (Sanastokeskus TSK 2017; Jantunen 2015). Suojelupoliisin vuosikirjoissa informaatiovaikuttaminen mainitaan kuitenkin usein nimenomaan hybridivaikuttamisen yhteydessä puhuttaessa esimerkiksi informaatiokampanjoista (ks. myös alaluku 3.1). Informaatiovaikuttamista koskevat ensimmäiset suorat maininnat ovat vuosikirjoissa lyhyitä ja liittyvät usein ulkovaltojen toimintaan: vuosien 2016 ja 2017 vuosikirjoissa ulkomaisen tiedustelun kohteiksi mainitaan Suomen toimet "informaatiovaikuttamiselta suojautumiseksi" (Supo, 2016; 2017). Etenkin verkon kautta tapahtuva informaatiovaikuttaminen näyttäytyi uhkana sen takia, että sen ennakointi on entistä haastavampaa.

Informaatiovaikuttaminen nähdään uhkana myös toisesta näkökulmasta: vuosikirjojen mukaan vieraiden valtioiden tiedusteluorganisaatiot ovat yrittäneet hankkia avustajiksi henkilöitä, joiden avulla olisi mahdollista vaikuttaa suoraan tai välillisesti joko poliittiseen päätöksentekoon ja yleiseen mielipiteeseen (Supo, 2018b). Informaatiovaikuttamisen keinoin voidaan siis vaikuttaa suoraan demokraattisen järjestelmän perusteisiin sekä laajemmasta näkökulmasta katsottuna myös valtion johtoon. Tällöin uhaksi nousisi erityisesti suomalaista järjestelmää ja päätöksentekijöitä kohtaan tunnetun luottamuksen rapautuminen.

Kuten yllä on todettu, informaatiovaikuttamiseen ja sen seurauksiin liittyvä tematiikka on noussut vuosikirjoissa enemmän esille 2020-luvun alussa. Taustalla näyttäytyy muun muassa Venäjän ja Kiinan aktiivinen toiminta länsimaita ja niiden arvoja vastaan. Kokonaisuudessaan informaatiovaikuttaminen ja sen mahdolliset konkreettiset seuraukset jäävät varsin vähäisille maininnoille vuosikirjoissa verrattuna useisiin edellä esiteltyihin uhkakuviin. Mahdollisesti eräs syy on se, että informaatiovaikuttaminen ei ole Suomessa kriminalisoitua. Suomen lainsäädäntö ei kaikilta osin vastaa nykyistä tiedonvälitysympäristöä, minkä myös Suojelupoliisi on julkisuudessa tunnustanut haasteeksi (Yle 6.8.2022).

Vuosikirjoista poiketen kansallisen turvallisuuden katsauksissa kuvataan suoremmin ulkovaltojen vaikuttamistoiminnan uhkaa ja mahdollisia toimijoita. Vaikuttamistoimintaa harjoittavat nimenomaan autoritaariset valtiot, joiden tavoitteena on levittää omia etujaan edistävää sisältöä tiedotusvälineissä ja sosiaalisessa mediassa. Näin pyritään vaikuttamaan päättäjien ja kohdemaassa olevien diasporayhteisöjen ajatteluun. Tällaisen ulkovaltojen harjoittaman toiminnan odotettiin jatkuvan laajamittaisena

epävarmuustekijöiden ja erilaisten jännitteiden lisääntyessä maailmanpolitiikassa (Supo, 2021a).

4 Terrorismi, radikalisoituminen ja ääriliikkeiden uhka

Suojelupoliisin 2015–2022 julkaisemissa vuosikirjoissa ja kansallisen turvallisuuden katsauksissa terrorismi saa laajasti huomiota. Vähittäisen uhan kehittymisen voi havaita jo vuosien 2010–2014 vuosikertomuksista. Suojelupoliisin julkaisujen mukaan uhka on moninainen ja siihen liittyy kiinteästi kansainvälisen tilanteen muutokset ja tapahtumat konfliktialueilla, esimerkiksi Syyriassa ja Irakissa. Kansainvälisen ulottuvuuden vuoksi terrorismia torjutaan, jotta Suomesta ei muodostuisi olennaisesti heikompi tai otollisempi kohde terrorismille, ja jotta kansainväliset yhteistyömahdollisuudet terrorismin torjumisessa pysyisivät auki (Kullberg, 2011).

Terrorismin määritelmästä ei ole yksimielisyyttä. Sen ajatellaan kuitenkin kattavan väkivaltaisen toiminnan, joka kylvää kauhua, pelkoa tai levottomuutta ja jolla on poliittinen tai uskonnollinen motiivi. (Moilanen, 2022; Schmid, 2004) Se, mikä ymmärretään terrorismiksi tai poliittiseksi väkivallaksi ja minkälainen asema niillä on yhteiskunnassa, on vaihdellut ajasta ja paikasta toiseen (Tammikko, 2019). Terrorismi on Suomessa nähty ennen kaikkea kansainvälisenä ilmiönä (Moilanen, 2022). Ääriliikkeet taas on tyypillisesti yhdistetty kotimaiseen äärioikeistoon ja joskus äärivasemmistoon, jotka saavat kansainvälisiä vaikutteita. Näihin liikkeisiin saattaa liittyä kulttimaisia ympäristöjä, eräänlaisia yhteiskunnan arvoja vastustavia ajatushautomoja, joissa myös kumouksselliset ja väkivaltaiset ideologiat kehittyvät. (Tammikko, 2019) Radikalisoituminen taas voidaan nähdä kognitiivisena ja käyttäytymiseen liittyvänä prosessina, jossa yksilö alkaa hyväksyä ja jopa ihannoida väkivaltaa keinona kukistaa vastustajat saavuttaakseen omat päämääränsä (Moilanen, 2022; Nilsson, 2018). Radikalisoituminen ei kuitenkaan aina johda vakaumuksen väkivaltaiseen toteuttamiseen (Nilsson, 2018).

4.1 Terrorismi ja radikalisoituminen

Vielä 2010-luvun alkupuolella terroritekojen uhka näyttäytyi vähäisenä, vaikka kansainvälinen terrorismi oli ujuttautunut jo Pohjoismaihin (Supo, 2010). Syyskuussa 2011 käynnistyi Suomen ensimmäinen terrorismirikoksen esitutkinta, jossa tutkittavilla ilmeni yhteyksiä Somalian al-Shabaabin tukemiseen. Kansainvälinen yhteistyö oli vilkasta terrorismin torjunnan toimintaympäristön muuttuessa yhä haastavammaksi sekä taustalla vaikuttavien ideologioiden, järjestöjen ja kohdehenkilöiden lukumäärän kasvaessa. (Supo, 2011; 2012) Taistelukokemusta hankkineet, konfliktialueilta palaavat jihadisteveteraanit työllistivät turvallisuusviranomaisia Euroopassa. Uudenlainen tilanne vaati Suomessakin terrorismintorjunnan strategian päivitystä ja kansainvälisen yhteistyön tiivistämistä. (Supo, 2013) Vuonna 2014 yksittäisten iskujen uhan arvioitiin kohonneen, vaikka Suomea ei pidetty väkivaltaisten radikaali-islamististen tai muidenkaan terroristijärjestöjen ensisijaisena kohteena (Supo, 2014).

Marraskuussa 2015 Supo arvioi yksittäisten iskujen uhan kohonneen ja monimuotoistuneen, mutta piti suunnitelmallisten iskujen uhkaa edelleen matalana. Toimintaympäristön todettiin muuttuneen: Suomeen arveltiin muodostuneen terroristista toimintaa tukevia rakenteita. (Supo, 2015) Suojelupoliisi ennakoi mahdollisia

pitkäaikaisvaikutuksia, sillä terroristijärjestöjen hallinnoimilla Syyria-Irakin alueilla oli kasvamassa uusi jihadistisukupolvi, jolla oli kytköksiä Suomeen (Supo, 2016).

Radikaali-islamistisen voimakkaan länsivastaisen ja jihadismiin pyrkivän propagandan levittäminen alkoi keskittyä ammattimaisen propagandan sijaan vaikeasti valvottaviin pikaviestipalveluihin. Kesällä 2017 Supo otti julkiseen käyttöön neliportaisen asteikon terrori-iskun uhan tason viestimiseen. Kesäkuussa 2017 uhka asettui tasolla kaksi eli ”kohonnut”. Terrorismin uhan kuvattiin olevan korkeampi kuin koskaan aiemmin. Muutamaa kuukautta myöhemmin, elokuussa 2017, tapahtui Suomen ensimmäinen terrori-iskuksi luokiteltu teko, puukotusisku Turussa. (Supo, 2017)

Juhlavuosikirja 2018 käsitteli maailmanlaajuisia megatrendejä peilaten niitä uhkakuviin. Maailmanlaajuisten epävakauttavien megatrendien, kuten ilmastonmuutoksen, resurssipulan ja väestörakenteen muutosten, todettiin tarjoavan kasvualustaa konflikteille ja radikalisoitumiselle ja siten vaikuttavan terrorismiin ilmiönä myös Suomessa. Viholliskuvien rakentamisen, syrjäytymisen ja poliittisen haurauden taas arveltiin kasvattavan entisestään vastakkainasettelua väestöryhmien välillä ja ruokkivan radikaalien ideologioiden suosiota. Radikaali-islamistisen terrorismin arvioitiin jatkossakin olevan Suomen kansalliseen turvallisuuteen eniten vaikuttava terrorismin muoto. Teknologisen kehityksen ennustettiin tarjoavan terroristisille toimijoille laajasti uusia mahdollisuuksia, vaikka perinteisemmät yksinkertaiset toimintatavat säilyttävätkin paikkansa helpon toteutettavuutensa vuoksi. Vaikka vuonna 2018 ei merkittäviä muutoksia tapahtunut edelliseen vuoteen verrattuna, kokonaisuudessaan terrorismin uhan todettiin kasvaneen radikaali-islamistisen ideologian levittäytyessä ja radikalisaation syvetessä (Supo, 2018)

Vuonna 2019 terrorismin tilannekuvan ja toimintakentän todettiin muuttuneen Suomessa ja kansainvälisesti. Konfliktialuematkailu voimistui ja verkostoituminen lisäsi kykyä ja valmiutta väkivaltaan (Supo, 2019). Uusi vuosikymmen toi voimistuneen äärioikeistolaisen terrorismin uhan sekä Suomessa että muualla länsimaissa. Äärioikeistolaisen terrorismin uhan nähtiin keräävän voimaa yhteiskunnallisista vastakkainasetteluista ja iskuista inspiroitumisesta. Laajamittaisen väkivallan kohteina olivat etniset ja uskonnolliset vähemmistöt, vähemmistöuskontojen symboliset kohteet sekä liberaalia maahanmuuttopolitiikkaa kannattavat poliitikot. (Supo, 2020)

Pandemia-aika lisäsi verkossa vietettyä aikaa ja loi näin kasvualustaa radikalisoitumiselle. Äärioikeistolainen terrorismi nousi keskiöön, kun Kankaanpäässä pidätettiin loppuvuodesta 2021 viisi henkilöä. Sosiaalisen median tukemana on muodostunut löyhiä kansainvälisiä yhteisöjä, joissa globaaleja ilmiöitä ovat muun muassa rotusotaa ja yhteiskunnan romuttamista kannattavat akselerationismi sekä Siege-kulttuuri. Uudeksi nousevaksi kansainväliseksi ilmiöksi nostettiin alaikäisten kasvava osuus niin ääri-islamisessa kuin äärioikeistolaisessa terroristisessa toiminnassa. (Supo, 2021).

Vuoden 2022 kansallisen turvallisuuden katsauksessa kuolonuhreja vaatineiden terrori-iskujen määrän todettiin länsimaissa laskeneen 2010-luvun puolivälistä. Terrorismin uhkataso pysyy kuitenkin neliportaisen asteikon tasolla kaksi, “kohonnut”. Venäjän hyökkäyssodan Ukrainassa ei merkittävästi uskottu vaikuttaneen terrorismin uhkaan Suomessa tai muualla länsimaissa. (Supo, 2022a) Radikaali-islamistisen toiminnan arvioitiin keskittyvän enimmäkseen tukitoimintoihin, kuten varainkeruuseen, värväämiseen sekä propagandan levittämiseen (Supo, 2022b). Vaikeasti torjuttavimmin ja merkittävimmän uhan muodostivat edellisvuosien tapaan yksittäiset toimijat ja salassa toimivat pienryhmät. Laajamittaisia vahinkoja ja tuhoja pyrkivät edelleen aiheuttamaan radikaali-islamistiset ja äärioikeistolaiset toimijat. (Supo, 2022a)

4.2 Ääriliikkeet

Ääriryhmä on ryhmä yksilöitä, joiden arvot, ihanteet ja uskomukset eroavat yhteiskunnan normaalina pitämistä vastaavista. Ääriryhmät saattavat käyttää väkivaltaisia keinoja välittää sanomaansa ulkopuolisille. Näin ollen monet keskustelut ääriryhmistä korreloivat terrorijärjestöistä käytävien keskusteluiden kanssa. (Norwood, 2022) 2010-luvun alkupuolella ääriliikkeiden toiminta oli vähäisesti esillä (Supo, 2011; 2012). Norjan iskujen (Oslo ja Utøya) myötä äärioikeistolaisten ryhmien valmius väkivaltaiseen toimintaan nousi Suomessakin julkiseksi puheenaiheeksi. (Supo, 2011) Suomessa ei ollut 2010-luvun puoliväliin mennessä tapahtunut ääriliikkeiden terroritekoja (Supo, 2014).

Turvapaikanhakijoiden määrän huomattava kasvu kiristi yhteiskunnallista ilmapiiriä vuonna 2015 ja aktivoi järjestäytynyttä ääriliikehdintää. Äärioikeistolaiset ryhmät vastustivat maahanmuuttoa näkyvästi ja vihapuheella lietsoen (Supo, 2015). Vaikka pelko turvallisuuden heikentymisestä oli esillä vahvasti vuonna 2015, maahanmuuttovastainen kiristynyt yhteiskunnallinen ilmapiiri ja protestiliikehdintä vähenivät vuosina 2016-2017, eivätkä ne vaarantaneet kansallista turvallisuutta (Supo, 2016; 2017). Seuraavina vuosina ääriliikkeiden toiminta näyttäytyi enimmäkseen äärioikeistolaisena katuväkivaltana ja äärivasemmistolaisten vahingontekoina. (Supo, 2018b; 2019) Vuoden 2018 vuosikirjassa ennakoitiin äärioikeistolaisen, väkivaltaan sallivasti suhtautuvan piirin vaikuttavan Suomen turvallisuustilanteeseen jatkossa (Supo, 2018b).

Vuoden 2020 vuosikirjassa tapahtui käänne, jossa äärioikeistolainen toiminta nostettiin voimakkaammin terrorismin uhaksi. Rajat ääriliikkeiden ja terrorismin välillä hämärtyivät. Verkossa muhiva radikalisoituminen muutti nopeasti Suomen äärioikeistoa. Iskuja pyrkivät tekemään yksittäiset toimijat ja pienryhmät järjestäytyneen äärioikeistoliikehdinnän menettäessä näkyvyyttään. Äärioikeistolaisen aatteen keskeisiä lähtökohtia – maahanmuuttovastaisuutta, muukalaisvihamielisyyttä sekä valkoisen identiteetin suojelua – täydennettiin eri piireissä mitä moninaisimpia vakaumuksia yhdistellen ja ideologioiden rajaviivoja haalentaen. (Supo, 2020b; 2021b).

Vuoden 2022 kansallisen turvallisuuden vuosikatsauksessa todetaan Venäjän hyökkäyssodan Ukrainassa herättäneen ääritoimijoiden kiinnostusta. Erityisesti äärioikeistolaisia vapaaehtoisia on matkustanut länsimaista Ukrainaan osallistuakseen aseelliseen toimintaan tai esimerkiksi materiaalisen tuen toimittamiseen. Onkin mahdollista, että sota kohottaa suomalaisen äärioikeiston väkivaltakyvykkyyttä. (Supo, 2022a)

Edellä esitetyt terroristisen toiminnan, radikalisoitumisen ja ääriliikehdinnän kaltaiset uhat korostuvat Suojelupoliisin vuosikirjoissa, mutta myös muunlaisia ryhmiä ja ideologista liikehdintää mainitaan. Esimerkiksi vuoden 2016 vuosikirjassa sivutaan Suomen ydinvoiman vastaista radikaaliliikehdintää ja pitkään uinuneen eläinoikeusaktivismin uudelleen heräämistä (Supo, 2016). Vuonna 2022 terrorismin uhka kumpusi edelleen yksittäisten henkilöiden ja salassa toimivien pienryhmien äärioikeistolaisesta sekä radikaali-islamistisesta ideologiasta (Supo, 2022a).

5 Pakolaisvakoilu

Pakolaisvakoilulla tarkoitetaan toimintaa, jossa vieraiden valtioiden tiedustelupalvelut pyrkivät kontrolloimaan Suomessa pysyvästi asuvia tai tilapäisesti oleskelevia

kansalaisiaan (Supo, 2011). Oikeusministeriön lainvalmisteluosaston vuoden 2013 arviomuistiossa pakolaisvakoilu määritellään toiminnaksi, jolla vierasta valtiota hyödyttäviä tietoja hankitaan kohdehenkilön olosuhteista, poliittisista mielipiteistä tai muista vastaavista seikoista (Oikeusministeriö, 2013). Keskeistä tässä pakolaisvakoilun kuvauksessa on se, että toiminnasta aiheutuu vaaraa kohdehenkilölle tai hänen läheiselleen heidän joutuessaan vainon tai painostuksen kohteeksi rotunsa, uskontonsa, poliittisten mielipiteidensä tai vastaavien syiden takia. Suojelupoliisi toteaa pakolaisvakoilun kohdistuvan ulkomailla oleviin toisinajattelijoihin, pakolaisiin tai ihmisoikeusaktivisteihin. Tämä toiminta voi johtaa vakoilun kohteena olevan läheisten häirintään, pidätyksiin, kuulusteluihin sekä pahimmillaan kidutuksiin ja kuolemanrangaistuksiin heidän kotimaassaan (Supo, 2011). Toiminnan tarkoituksena voi olla kohdehenkilön (esim. toisinajattelijan) toiminnan kartoittaminen sekä pyrkimys saada kohde luopumaan mahdollisista kotimaansa hallitusta vastustavista toimista uhkailun ja propagandan keinoin (Oikeusministeriö, 2013). Suojelupoliisi on todennut pakolaisvakoilun vaarantavan valtion turvallisuutta sekä loukkaavan Suomen kansalaisten ja muiden Suomessa pysyvästi oleskelevien perusoikeuksia (Supo, 2018b).

Pakolaisvakoilua ei ole kriminalisoitu Suomessa, kuten Ruotsissa ja Norjassa, mutta Suojelupoliisi esitti vuoden 2012 alussa tätä säädettävän rangaistavaksi (Supo, 2012). Myös esimerkiksi Vihreiden kansanedustaja Inka Hopsu on jättänyt asiasta toimenpidealoitteen Eduskunnalle vuonna 2020 (Eduskunta TPA 75/2020 vp), joten asia on laajemminkin huolenaiheena. Vuoden 2019 voimaan tulleen tiedustelulainsäädännön muutos näkyy myös pakolaisvakoilun torjunnassa: “Suojelupoliisi voi nykyään hankkia tietoa pakolaisvakoilusta ilman rikosepäilyä, jos konkreettinen kansallisen turvallisuuden uhka on olemassa” (Supo, 2021b, 6).

Jo Suojelupoliisin vuoden 2011 vuosikertomuksessa todettiin pakolaisvakoilutapauksia ilmenneen enemmän kuin aikaisempina vuosina (Supo, 2011) ja tarkastelujakson vuosikirjoissa ilmiö onkin todettu pysyväksi. Pakolaisvakoilusta ei ollut mainintaa vuosina 2019 ja 2020, mutta vuoden 2021 vuosikirjassa se tuotiin jälleen esille aikaisempaa laajemmassa katsauksessa sekä kuvitteellisessa tyyppiesimerkissä. Vuosikirjoissa korostuu toistuvasti kriminalisoinnin puuttuminen ja tarve lisätä tämä yleisen syytteen alaiseksi rikokseksi (Supo, 2021b). Vaikka tapauksia on ilmennyt, mahdollisesti vain yksittäisiä tapauksia tulee lopulta esille – osasyynä tälle on arvioitu olevan, että teot eivät useinkaan tule poliisin tai Suojelupoliisin tietoon asianomistajiin kohdistettujen uhkausten vuoksi (Oikeusministeriö, 2013).

Pakolaisvakoilun ohella vuosikirjoissa mainitaan Suomessa asuvat kaksoiskansalaiset ja se, että ulkovallat saattavat käyttää heitä hyödyksi eri tavoin. Suojelupoliisi on arvioinut, että kaksoiskansalaisuuteen saattaa sisältyä riskejä tiedusteluntorjunnan näkökulmasta. Kansallisen turvallisuuden näkökulmasta kaksoiskansalaisuus voi muodostua uhaksi: vieraat valtiot saattavat kohdella kaksoiskansalaisia vain omina kansalaisinaan ja esimerkiksi virkamiesten painostamisessa on pyritty käyttämään hyväksi heidän sidonnaisuuksiaan kyseisiin valtioihin ja niiden kansalaisiin. Esimerkiksi Venäjän kansalaiset ovat kaksoiskansalaisuudesta riippumatta Venäjän lakien mukaan velvoitettuja auttamaan venäläisiä turvallisuusviranomaisia. (Supo, 2016)

6 Yhteiskuntaan kohdistuvat laaja-alaiset uhat: Kohteena kriittinen infrastruktuuri sekä yritys-, tiede- ja tutkimustoiminta

Kriittisellä infrastruktuurilla tarkoitetaan julkishallinnon organisaatioita ja yrityksiä, jotka ylläpitävät ja rakentavat muun muassa energiahuoltoa, tietoliikenneverkkoja ja vesihuoltoa. Nämä ovat mahdollisia kohteita valtiollisille vakoilijoille. Infrastruktuurin rakenne ja turvallisuusjärjestelyt ovatkin yksi kohde Suomeen kohdistuvalle tiedustelulle, jonka pyrkimyksenä on selvittää Suomen sotilaallisen valmiuden lisäksi yhteiskunnan kriisinsietokykyä ja huoltovarmuutta (Supo, 2016). Vuosikirjoissa esille tulevia keskeisiä ulkomaisen vakoilun kiinnostuksen kohteita kriittisen infrastruktuurin osalta ovat esimerkiksi energiahuoltovarmuus ja Suomen kyberturvallisuusrakenteet (Supo, 2016). Vakoilun tarkoituksena ei ole niinkään tietojen anastaminen tiedustelukohteista vaan kartoittaa kriittisen infrastruktuurin järjestelmistä haavoittuvuuksia ja ominaisuuksia, joilla nämä voitaisiin kriisitilanteessa lamauttaa (Supo, 2017). Kriittisen infrastruktuuriin kohdistuvan vakoilun torjunnan todetaan olevan haastavaa: yksityisten yritysten merkitys kasvaa koko ajan ja kriittinen infrastruktuuri onkin nykyisin lähes kokonaan yksityisessä omistuksessa (pl. vesihuolto ja liikenne). Lainsäädännön näkökulmasta yksityiseen elinkeinonharjoittajaan kohdistuva oikeudeton tiedonhankinta on asianomistajarikos, jota ei katsota valtioon kohdistuvaksi vakoiluksi ja näin ollen se ei myös aina mahdollista riittävien tiedonhankintakeinojen käyttöä. (Supo, 2017).

Tarkasteluvuosina kriittiseen infrastruktuuriin kohdistuneet uhat olivat jatkuvasti esillä, ja niiden tärkeys korostui uusimmissa vuosikirjoissa muun muassa yhteiskunnan digitalisoitumisen edetessä (Supo, 2021b. Ks. myös alaluku 3.2). Kybervakoiluntorjunta on todettu vaikeaksi, mutta ennaltaehkäisykeinona koulutetaan kriittistä infrastruktuuria ylläpitäviä ja huoltovarmuuteen liittyviä yrityksiä (Supo, 2018b). Toisena esimerkkinä torjuntakeinosta voidaan pitää turvallisuusselvitysten tekoa, joka kuuluu pääosin Suojelupoliisille (Supo, 2021b).

Vuosikirjoissa kriittiseen infrastruktuuriin kohdistuvien uhkien tarkastelu limittyy usein taloudellisten teemojen kuten yritysmaailmaan kohdistuvien uhkien käsittelyyn. Kriittisen infrastruktuurin ollessa Suomessa monin osin kuntien tai yksityisten omistuksessa ja siten myös sidoksissa niiden taloustilanteeseen, on mahdollista että infrastruktuuri joutuu myös alttiiksi ulkomaisten toimijoiden riskialttiille investointi- tai ostoyrityksille (Supo, 2019; 2020b).

Vuosikirjojen mukaan ulkomaisten toimijoiden kiinnostus on kohdistunut Suomessa yritysten lisäksi tiede- ja tutkimustoimintaan sekä niiden hallussa olevaan tietoon. Niiden kohdalla uhkakuvat ovat muuttuneet pysyvästi digitalisaation myötä: käytännössä uhat ovat monimuotoistuneet ja näköpiiriin on noussut uudenlaisia uhkatekijöitä aivan samalla tavoin kuin useiden muiden yllä käsiteltyjen ilmiöiden kohdalla. Uusista uhkista vuosikirjoissa mainitaan yritysten alihankinta- ja palvelutuottajaketjuihin kohdistuvat verkkohyökkäykset, joilla pyritään hankkimaan pääsy tiedustelun varsinaisen kohteeseen (Supo, 2019). Keskinäisriippuvuuksien maailmassa uhaksi on noussut myös se, että yhteen toimijaan tai kohteeseen kohdistunut uhka voisi vaikuttaa toiseenkin (Supo, 2021b).

Hyökkäysten, vaikuttamisen ja vakoilun kohteina mainitaan etenkin tuotekehitystyötä tekevät yritykset ja niille palveluita tarjoavat yritykset. Yritysvakoilua on kohdistunut hyvinkin erilaisiin toimialoihin kuten esimerkiksi elektroniikka-, laiva- ja energiateollisuuteen sekä terveysteknologia-alaan. Tämänkaltaisen toiminnan taustalla esitettiin

olevan usein valtiollinen taho, joka tavoitteli käyttöönsä yritysten tuotekehittelyssä luotua tietoa ja osaamista vähällä panoksella ja matalalla riskillä. (Supo, 2016; 2017). Samalla tavoin yliopistojen ja tutkimuslaitosten tieteellis-tekninen tutkimustyö ja toiminta on ollut vieraiden valtioiden tiedustelun kohteena (Supo, 2021b). Tiede- ja tutkimustoimintaan kohdistuvat uhat korostuvat uusissa vuosikirjoissa, mikä kuvastaa turvallisuusympäristön muutosta.

Tarkastelujakson alussa yritysvakoilua harjoittavia tahoja ei mainittu suoraan, joten on huomionarvoista, että uusimmissa julkaisuissa nimetään suoraan tätä toimintaa harjoittavat valtiot eli Venäjä ja Kiina. Molempien maiden toimintaan on kiinnitetty huomiota mediassa ja tiedemaailmassa: Kiinan käyttämiä laittomia toimintamenetelmiä on tarkastelu esimerkiksi ase- ja muun teknologian kohdalla (Gilli & Gilli, 2019; Holt 2020). Kiinan hegemoniapyrkimykset talouden, teknologian ja globaalin infrastruktuurin rakentamisen saralla ovat kiristäneet maan suhteita länsivaltoihin, mikä heijastuu globaaliin tilanteeseen (Weil 2020; Frankopan 2022).

Venäjän ja Kiinan tiedustelullista kiinnostusta Suomea kohtaan on lisännyt suomalainen arktisen alueen olosuhdeosaaminen ja alueelle suunnitellut hankkeet. Venäjän kiinnostusta arktista aluetta kohtaan lisää luonnollisesti se, että alueesta noin puolet kuuluu Venäjään, joten maan arktista aluetta koskeva tiedon tarve on siis pysyvä. Myös Kiina tavoittelee alueella taloudellisia etuja kuten luonnonvaroja sekä merireitin ja logistiikan tarjoamia etuja (Supo, 2018b; 2019). Molempien valtioiden kohteina ovat – sotilaallisen toiminnan ohella – erilaiset merikaapeli- ja satelliittiasemahankkeet ja muut teknologiaprojektit. Kiinnostuksen kohteena mainitaan olleen myös koillisväylän merikaapelihanke, jonka oli tarkoitus yhdistää Eurooppa ja Aasia (Supo, 2019). Kansainvälisen ilmapiirin kiristyttyä hanke joutui vastatuuleen (HS, 29.10.2022).

7 Lopuksi: muuttuva toimintaympäristö luo monimuotoisia uhkia

Suojelupoliisin vuosikirjoissa uhkakuvat muuttuivat monimuotoisimmiksi vuosien 2015–2021 aikana, minkä esitetään johtuvan epävarmemmasta ja vaikeammin ennakoitavasti toimintaympäristöstä. Muutosten taustalla vaikuttavat osin laaja-alaiset globaalit kehityssuunnat eli megatrendit, kuten ilmastonmuutos, väestönkasvu, muuttoliike ja teknologian kehitys, mutta myös kansallisen tason muutokset, kuten verkkoympäristön nopean muutos ja informaatioon liittyvät riskit, joilla on vaikutusta Suomen kansalliseen turvallisuuteen.

Yhteistä monille uhkakuville on se, että ne liittyvät yhteiskunnan kannalta keskeisiin toimintoihin, demokraattisen järjestelmän rakenteisiin tai poliittisiin päätöksentekijöihin ja päätöksentekoon. Yleisiin asenteisiin, mielipiteisiin ja päätöksiin vaikuttaminen informaatio-, kyber- ja hybridivaikuttamisen keinoin nousi vuonna 2022 ajankohtaiseksi Nato-keskustelun myötä. Suoraan valtionjohtoon kohdistuvat uhat mainitaan harvemmin, kun taas ulkovaltojen eri menetelmin päätöksentekoon ja kansalaismielipiteeseen kohdistama vaikuttaminen tulee esille toistuvasti. Laajasti ymmärrettynä uhat kohdistuvat usein suomalaisen yhteiskunnan eri osa-alueisiin ja suomalaista järjestelmää tai päätöksentekoa kohtaan tunnettuun luottamukseen.

Terrorismin uhka ja sen torjunnan tarve korostuivat tarkastelujaksolla. Taustatekijöiksi on esitetty muun muassa toimintaympäristön muutosta, joka tapahtui Syyrian-Irakin alueiden konfliktien takia sekä Venäjän Ukrainaa vastaan kohdistamien toimien seurauksena. Vuotta 2017 voidaan pitää käännekohtana ensimmäisen Suomessa

tapahtuneen terrori-iskun takia. Vuosikirjojen mukaan myös ääriliikkeiden toiminnan ja terrorismin raja muuttui häilyvämmäksi. Verkkoympäristö ja pikaviestipalvelimet ovat tulleet yhä keskeisemmiksi alustoiksi ideologioiden leviämisessä, radikalisoitumisessa ja aatemaailmojen hajaantumisessa. Tämä tekee uhkien ennakoinnista haastavampaa jatkossakin.

Myös vieraiden valtioiden harjoittama vaikuttaminen on ilmiönä monipuolistunut: vuosikirjojen mukaan se ei enää nykyisin kata ainoastaan laitonta tiedustelua, vaan sisältää monenlaisia vaikuttamiskeinoja, joita on usein vaikea tunnistaa ja joiden tekijää on vaikea varmuudella identifioida. Valtiollisen vaikuttamisen arvioidaan todennäköisesti lisääntyvän, sillä useat valtiot pyrkivät kasvattamaan valtaansa, mutta haluavat välttää suoraa sotilaallista konfliktia. Vaikutuskeinot eivät kohdistu ainoastaan suomalaisiin, vaan myös muu Suomessa pysyvästi oleskeleva tai esimerkiksi Suomesta turvapaikkaa hakeva saattaa joutua kotimaansa vakoilun kohteeksi (pakolaisvakoilu). Tämä vakoilun muoto ei ole kriminalisoitu Suomessa, mutta Suojelupoliisin lisäksi muutkin tahot ovat ajaneet toiminnan saattamista yleisen syytteen alaiseksi rikokseksi jo useamman vuoden ajan. Tästä voidaan päätellä asian olevan tärkeä, mutta myös oikeudellisesti haastava (ks. Oikeusministeriön 2013 arviomuistio)

Huomionarvoinen muutos on, että uusimmissa vuosikirjoissa nimetään suoraan ne valtiot, jotka harjoittavat laitonta tiedustelua tai toimivat muutoin kyseenalaisesti kansainvälisessä toimintaympäristössä. Erityisesti Venäjän ja Kiinan harjoittama Suomen kansallista turvallisuutta uhkaava tiedustelu nousee esille 2020-luvun alun vuosikirjoissa ja katsauksissa. Näiden valtioiden aktiivisuuden on esitetty pysyvän korkeana. Perinteisen henkilötiedustelun rinnalle on tullut aiempaa aktiivisempi kybervakoilu. Suomeen kohdistuu jatkuvia kybervakoiluyrityksiä, eikä toiminnan odoteta laantuvan pitkälläkään aikavälillä. Koronapandemian siirrettyä monia toimintoja verkkoon myös kybervakoilulle avautui uusia vaikutusmahdollisuuksia.

Kriittiseen infrastruktuuriin kohdistuvat uhat korostuivat vuosikirjoissa useista syistä. Esimerkiksi yksityisen sektorin kasvanut rooli kriittisen infrastruktuurin omistajana nousi keskeiselle sijalle. Erityisesti lainsäädännöllisten syiden mainitaan aiheuttavan haasteita kriittiseen infrastruktuuriin liittyvien uhkien ennaltaehkäisyssä. Lisäksi esille nousivat yritys-, tiede- ja tutkimustoimintaan liittyvät uhat, kuten vakoilu ja kyberhyökkäykset. Tässäkin yhteydessä autoritaariset maat mainittiin aktiivisina toimijoina.

Nykyisissä turvallisuuskeskusteluissa toistuu käsite “uusi normaali”. Uudessa normaalissa toimintaympäristö kuvataan epävakaaksi, epävarmaksi, monimutkaiseksi ja monimerkitykselliseksi. Toimintaympäristön muutosnopeus ei tule hidastumaan, vaan tulevaisuus näyttäytyy yhä epäselvempänä ja vaikeammin ennakoitavana (Limnéll & Iloniemi 2018). Tämä havainto näyttää olevan yhtäläinen Suojelupoliisin vuosikirjoissa esitettyjen tietojen kanssa. Niin sanotun “uuden normaalin” aikakaudella uhkakuvat ovat muuttuvia ja yllättäviä. Viime aikoina ilmastoaktivismi on noussut esille eri puolilla Eurooppaa (Yle, 11.11.2022; HS, 24.10.2022). Uhkakuvien kehityksen kannalta on kiinnostavaa pohtia, voisiko ilmastonmuutos johtaa tulevaisuudessa poliittiseen väkivaltaan konfliktien syvetessä ja maltillisuuden loppuessa kuten esimerkiksi terrorismin tutkija Leena Malkki on esittänyt (Malkki, 2020). Tulevaisuuden terrorismin uhkakuviksi on esitetty myös verkko- ja ydinterrorismia sekä biologista ja kemiallista terrorismia. (Puistola & Herrala, 2006).

Lähteet

Althoff, M. (2016). Human Intelligence. Teoksessa Lowenthal, M. M. & Clark, R. M. (toim.), *The Five Disciplines of Intelligence Collection*, ss. 45-79. Thousand Oaks, California: CQ Press.

Eduskunta TPA 75/2020 vp. (2020). Toimenpidealoite pakolaisvakoilun kriminalisoimisesta. [Aloite]. Toimenpidealoite TPA 75/2020 vp. [viitattu 15.11.2022]. https://www.eduskunta.fi/FI/vaski/EduskuntaAloite/Documents/TPA_75+2020.pdf

Elinkeinoelämän keskusliitto (EK). (2018). Kybervakoilu − mitä jokaisen yrityksen tulisi tietää? [viitattu 19.11.2022]. https://ek.fi/ajankohtaista/uutiset/kybervakoilu-%E2%88%92-mita-jokaisen-yrityksen-tulisi-tietaa/.

Frankopan, P. (2022). *Uudet Silkkitiet. Tulevaisuuden maailmanhistoria*. Jyväskylä: Atena.

Gilli, A. & Gilli, M. (2019). Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage. *International Security*, 43, 141–189.

Haukkala, H. (2020). *Suuren pelin paluu: Suomen tulevaisuus kriisien maailmassa*. Helsinki: Kustannusosakeyhtiö Otava.

Helsingin Sanomat (24.10.2022). Kulttuuri. [verkkosivu]. Ilmastoaktivistit heittivät perunamuusia Monet'n teoksen päälle. [viitattu 17.11.2022]. https://www.hs.fi/kulttuuri/art-2000009155160.html.

Helsingin Sanomat (29.10.2022). Talous. [verkkosivu]. Suomalaisten haave arktisesta datakaapelista elää, vaikka Venäjän suunta umpeutui. [viitattu 15.11.2022]. https://www.hs.fi/talous/art-2000009160760.html.

Holt, A. (2020). A brief history of US-China espionage entanglements. [verkkoteksti]. MIT Technology Review 3.9.2020. [viitattu 17.11.2022]. https://www.technologyreview.com/2020/09/03/1007609/trade-secrets-china-us-espionage-timeline/

Jantunen, S. (2015). *Infosota: "iskut kohdistuvat kansalaisten tajuntaan*". Helsinki: Otava.

Kullberg, A. (2011). *Suomi, terrorismi, Supo : koira joka ei haukkunut : miksi ja miten Suomi on välttynyt terroristisen toiminnan leviämiseltä*? WSOY.

Laitinen, K., & Huhtinen, A. (2021). *Kansallinen turvallisuus murroksessa*. Docendo, Jyväskylä.

Limnéll, J. & Iloniemi, J. (2018). *Uhkakuvat*. Jyväskylä, Docendo.

Malkki, L. (2020). *Mitä tiedämme terrorismista*. Otava.

Moilanen, P. (2022). Terrorismi. Luento 3.11.2022. Turvallisuuden käsite ja sen muutos -luentosarja. Jyväskylän yliopisto.

Nilsson, Marco (2018) "Jihadiship: From Radical Behavior to Radical Beliefs", *Studies in*

Conflict and Terrorism. 1-17.

Norwood, M. (2022). Extremist Groups in Criminology: Definition & Overview. Study.com. [viitattu 20.11.2022]. https://study.com/academy/lesson/extremist-groups-definition-criminology-lesson.html

Oikeusministeriö (2013). Oikeusministeriön lainvalmisteluosaston arviomuistio 6.12.2013. Arviomuistio niin sanotun pakolaisvakoilun säätämisestä rangaistavaksi.

Puistola, J-A. & Herrala, J. (2006). *Terrorismi Euroopassa*. Tammi, Helsinki.

Sanastokeskus TSK. (2017). Kokonaisturvallisuuden sanasto. [verkkojulkaisu]. Helsinki: Sanastokeskus TSK ry. [viitattu 15.11.2022]. https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Kokonaisturvallisuuden_sanasto.pdf

Schmid, A. (2004). Terrorism - the definitional problem. *Case Western Reserve Journal of International Law*, 36(2-3), 375-419.

Simola, M. (Toim.) (2009). *Ratakatu 12: Suojelupoliisi 1949-2009*. Helsinki: WSOY.

Sisäministeriö (2019). Tiedote.[verkkosivu]. Laki siviilitiedustelusta voimaan kesäkuun alussa.[viitattu 15.11.2022]. https://intermin.fi/-/laki-siviilitiedustelusta-voimaan-kesakuun-alusta.

Suojelupoliisi (2010). *Suojelupoliisin vuosikertomus 2010.* Helsinki.

Suojelupoliisi (2011). *Suojelupoliisin vuosikertomus 2011*. Helsinki.

Suojelupoliisi (2012). *Suojelupoliisin vuosikertomus 2012*. Helsinki.

Suojelupoliisi (2013). *Suojelupoliisin vuosikertomus 2013*. Helsinki.

Suojelupoliisi (2014). *Suojelupoliisin vuosikertomus 2014*. Helsinki.

Suojelupoliisi (2015). *Suojelupoliisin vuosikirja 2015.* Helsinki.

Suojelupoliisi (2016). *Suojelupoliisin vuosikirja 2016.* Helsinki.

Suojelupoliisi (2017). *Suojelupoliisin vuosikirja 2017.* Helsinki.

Suojelupoliisi (2018a). *Kansallisen turvallisuuden katsaus 2018.* Helsinki.

Suojelupoliisi (2018b). *Suojelupoliisin vuosikirja 2018.* Helsinki.

Suojelupoliisi (2019). *Suojelupoliisin vuosikirja 2019.* Helsinki.

Suojelupoliisi (2020a). *Kansallisen turvallisuuden katsaus 2020*. Helsinki.

Suojelupoliisi (2020b). *Suojelupoliisin vuosikirja 2020.* Helsinki.

Suojelupoliisi (2021a). *Kansallisen turvallisuuden katsaus 2021*. Helsinki.

Suojelupoliisi (2021b). *Suojelupoliisin vuosikirja 2021.* Helsinki.

Suojelupoliisi (2022a). *Kansallisen turvallisuuden katsaus 2022*. Helsinki.

Suojelupoliisi (2022b). Terrorismin uhka-arvio. Terrorismin uhka-arvio on tilannekuva terrorismista. [viitattu 17.11.2022]. https://supo.fi/uhka-arvio.

Tammikko, T. (2019). *Vihalla ja voimalla: poliittinen väkivalta Suomessa*. Gaudeamus, Helsinki.

Weil, S. (2020). China's discourse on the belt and road initiative: a hidden threat to European security logic?, *Journal of Contemporary European Studies*, DOI: 10.1080/14782804.2022.2068516

Yle (6.8.2022). Suojelupoliisi ehdottaa: Valeuutisten tahallinen levittäminen vieraan vallan puolesta tulisi säätää rikokseksi. Saatavilla osoitteessa https://yle.fi/uutiset/3-12561484 (haettu 14.11.2022).

Yle (11.11.2022). Ilmastoaktivistit yrittivät liimata itsensä maailmankuuluun Huuto-maalaukseen Norjassa – poliisin mukaan kiinni otettujen joukossa suomalainen. Saatavilla osoitteessa https://yle.fi/a/74-20004424 (haettu 17.11.2022).

Informaatioteknologian tiedekunnan julkaisuja
No. 98/2023

ISBN 978-951-39-9603-1 (verkkoj.)
ISSN 2323-5004

JYVÄSKYLÄN YLIOPISTO