Kansalaisten tekemä CITINT ja sen vertautuminen valtiolliseen tiedusteluun

Iikka Pietilä, Katleena Kortesuo, Ulla Pohjanen, Mikko Tuominen

1 Johdanto

Viime aikoina on herännyt tarve uudelle termille *CITINT*, joka tarkoittaa kansalaisten toteuttamaa ei-valtiollista tiedustelua. CITINT-kirjainyhdistelmä koostuu sanoista *citizen* (tai vaihtoehtoisesti *civic*) ja *intelligence* (ks. esim. Steele, 2002; Teti, 2012; Pešek, 2023). Sanayhdistelmä on tuttu INT-lopustaan, jonka avulla on muodostettu vastaavia termejä monista muistakin tiedustelulajeista.

Tässä raportissa käsitteestä intelligence käytetään vapaata suomennosta tiedustelu, ja sitä käytetään sanan laajassa merkityksessä kuvaamaan toimintaa, organisaatioita ja päätöksenteon alaprosesseja (esim. McDowell, 2008). Tiedustelutiedolla viitataan tässä raportissa tiedustelulla tuotettuun sensoritason tietoon (data), käsiteltyyn ja analysoituun tietoon (informaatio) sekä tiedusteluprosessilla tuotettuihin johtopäätöksiin ja toimenpidesuosituksiin. Citizen merkitsee suomeksi kansalaista tai kansalaisia[1].

Käsitteellä tiedustelu voidaan tässä raportissa viitata myös sotilaalliseen, rikostutkinnalliseen ja liiketoimintatiedusteluun tai esimerkiksi katastrofin- ja kriisinhallinnan tueksi tuotettuun tietoon. Huomionarvoista on, että raportissa liikutaan tiedustelun strategisilla, operatiivisilla ja taktisilla tasoilla, sillä CITINTiin tukeutuvat päätelmät ja johtopäätökset voivat painottua näille eri tasoille. Tässä raportissa strateginen taso linkittyy erityisesti esimerkiksi valtiolliseen päätöksentekoon ja pitempään aikajänteeseen, operatiivinen taso puolestaan alueelliseen toimintaan ja keskipitkään aikajänteeseen, ja taktinen taso lähelle ruohonjuuritasoa, yksittäisiä toimijoita ja lyhyisiin aikajänteisiin päätöksenteossa. (Ks. esim. Kerttunen, 2007.)

Raportissa vertaillaan valtiollisen tiedustelun ja kansalaisten tekemän tiedustelun eroja niin roolien, resurssien, metodien, alustojen kuin lainsäädännönkin kannalta. Erityisesti lainsäädännön näkökulmasta erot ovat merkittäviä, ja ne riippuvat myös siitä missä roolissa kansalaiset tekevät tiedustelua. Kansalaiset saattavat tehdä tiedustelua esimerkiksi yksityishenkilöinä, vapaamuotoisissa harrastusryhmissä, järjestöissä, kaupallisissa yrityksissä ja freelance-ammateissa kuten tutkivina journalisteina.

CITINT eli citizen intelligence ei ole terminä vielä vakiintunut. Niinpä tässä raportissa pyritään määrittelemään termi, perustelemaan sen käyttötarve ja myös vertailemaan CITINTin käytännön toteutuksia ja eroja verrattuna valtiolliseen tiedusteluun.

[1] Väärinkäsitysten välttämiseksi huomattavaa on, että termillä *civic intelligence* voidaan viitata myös yhteiskunnallisen ja poliittisen osallistumisen (engl. *participation*, ks. esim. Pietilä, 2022) aktiviteetteihin, joissa esimerkiksi ratkotaan yhteistyössä jotakin rajattua poliittista ongelmaa deliberatiivisin keinoin. Tällainen civic intelligence on kuitenkin rajattu tämän raportin ulkopuolelle.

Raportin luvussa 2 käydään läpi CITINT-termin määritelmä ja sen suhde muihin tiedustelun käsitteisiin. Luvussa 3 keskitytään valtiollisen tiedustelun ja kansalaistiedustelun eroihin muun muassa resurssien, roolien ja metodien näkökulmasta. Luku 4 kertoo, mitkä lait voivat tulla sovellettavaksi kansalaistiedusteluun. Luvussa 5 esitellään erilaisia CITINT-toimijoita ja -työkaluja. Luvun 6 johtopäätöksissä huomio kiinnitetään erityisesti CITINT-toiminnan laajenemiseen sekä sen uhkiin, heikkouksiin ja mahdollisuuksiin.

2 Mitä CITINT on?

CITINT-lyhenne esiintyy Burken artikkelissa (2022), mutta sille ei anneta tarkkarajaista määritelmää. Artikkelin CITINT-esimerkissä kerrotaan Ukrainan valtion luomasta sovelluksesta, johon kuka tahansa tunnistettu kansalainen voi raportoida vihollishavainnoista ja ladata valokuvia Ukrainan puolustusvoimien avuksi (Burke, 2022). Kyseessä on siis valtion fasilitoima CITINT.

CITINT-termi esiintyy myös Laulajaisen, Taivalmaan, Vilénin ja Virtasen raportissa, jossa he jakavat ei-valtiollisen tiedustelutoiminnan viiteen osa-alueeseen toimijoittain: (1) kaupalliset tiedusteluyritykset, (2) rikollisjärjestöt ja terroristiorganisaatiot, (3) kansalais- ja avustusjärjestöt, (4) tutkijat, tutkivat journalistit, kansalaisjournalistit ja kansalaistiedustelu sekä (5) tiedustelu osana yritysten normaalia toimintaa (Laulajainen ym., 2023). Tässä jaottelussa Laulajainen, Taivalmaa, Vilén ja Virtanen luokittelevat CITINTin järjestäytymättömän vapaaehtoistoiminnan alle eli neljänteen ryhmään, lähteenään Burke (2022). Näin CITINTin tekijöistä rajataan pois muun muassa kaupalliset tiedusteluyritykset, rikollisjärjestöt, rekisteröityneet yhdistykset tai kansalaisjärjestöt. (Laulajainen ym., 2023.)

Laulajainen ym. (2023) esittämää viisiosaista jaottelua voi opponoida, koska artikkelissa listattujen toimijakategorioiden status on varsin tulkinnanvarainen ja osin päällekkäinen. Voisi väittää, että moni terroristiorganisaatio on samaan aikaan kansalaisjärjestö, joskin toki epäeettinen sellainen. Lasketaanko esimerkiksi Irish Republican Army (IRA) terroristijärjestöksi vai kansalaisjärjestöksi? IRAn historiassa on sekä fyysisen väkivallan vuosia että rauhallisempia vaikuttamisen vuosia (Arthur & Cowell-Meyers, 2023). Vaihtuuko status CITINTistä pois ja takaisin sen mukaan, mitä keinoja ryhmä on käyttänyt? Myös Malkki toteaa artikkelissaan, että terrorismin määritelmä on yhä häilyvä, eikä siitä ole yhteisymmärrystä (Malkki, 2014).

Voi myös pohtia, onko CITINT-käsitteen kannalta selkeää, jos sama henkilö voi vuorotellen olla tai olla olematta CITINT-toimija. Jos esimerkiksi yksittäinen CITINT-harrastaja perustaa yrityksen tai jos vapaa CITINT-ryhmittymä rekisteröityy yhdistykseksi, sen toiminta päätyy CITINTin ulkopuolelle. Jos yrittäjä toteuttaa yksittäisen tiedusteluoperaation harrastuksenaan, lopputulos olisi jälleen CITINTia.

Hyödyllisempi ja käyttökelpoisempi tapa määritellä CITINT olisi rajata se *ei-valtiolliseksi tiedustelutoiminnaksi*. Tämän määritelmän hyväksyy myös yksityisen Black Bird Group -tiedusteluryhmän perustajajäsen ja OSINT-asiantuntija Emil Kastehelmi (haastattelu 17.10.2023). Määritelmän mukaan CITINT-toimijoita voivat olla esimerkiksi kaupalliset yritykset, kansalaisjärjestöt, ammatilliset yhdistykset, yksittäiset aktiivit ja jopa rikollisjärjestöt.

2.1 CITINT osana tiedustelun taksonomiaa

Tiedustelun alalajeja voi luokitella eri perusteilla. Yksi luokittelun kriteeri on tiedustelutoiminnassa käytetty kanava, tekniikka tai tiedonhankintatapa (engl. *source*). Tätä käytetään Lowenthalin ja Clarkin esittelemässä viisiosaisessa jaottelussa HUMINT, GEOINT, MASINT, SIGINT ja OSINT, jossa HUMINT viittaa henkilötiedusteluun, GEOINT geospatiaaliseen tiedusteluun eli paikkatietoon liittyvään tiedusteluun, MASINT mittaus- ja tunnusmerkkitiedusteluun, SIGINT signaalitiedusteluun ja OSINT avointen lähteiden tiedusteluun (Lowenthal & Clark, 2015). Näiden kaikkien kohdalla tiedonhankintatapa tai -tekniikka määrittelee tiedustelulajin nimen.

Toinen kriteeri määritellä tiedustelun alalajeja on tiedustelun kohde. Esimerkiksi vastatiedustelu (CI) tarkoittaa toimintaa, joka on suunnattu vastustajan tiedusteluun (Lowenthal & Clark, 2015; Isokangas, 2023c). Liiketoimintatiedustelu taas on kohdistettu yritysten toimintaympäristöön, kilpailijoihin ja markkinatilanteeseen (Isokangas, 2023a). Vastaavasti taloudellinen tiedustelu FININT (engl. *financial intelligence*) kohdistuu taloustietoon ja rahaliikenteeseen (Walton, 2013).

Kolmas kriteeri luokitella tiedustelun tyyppejä on toteuttajan yhteiskunnallinen rooli ja oikeusasema. Suomessa esimerkiksi sotilastiedustelu on toimintaa, josta vastaa puolustusvoimat. Siviilitiedustelusta taas vastaa Suojelupoliisi. Rikostiedustelua tekee lainvalvontaviranomainen eli poliisi, ja vakavien tapausten kohdalla myös Suojelupoliisi. (Sisäministeriö, 2017.)

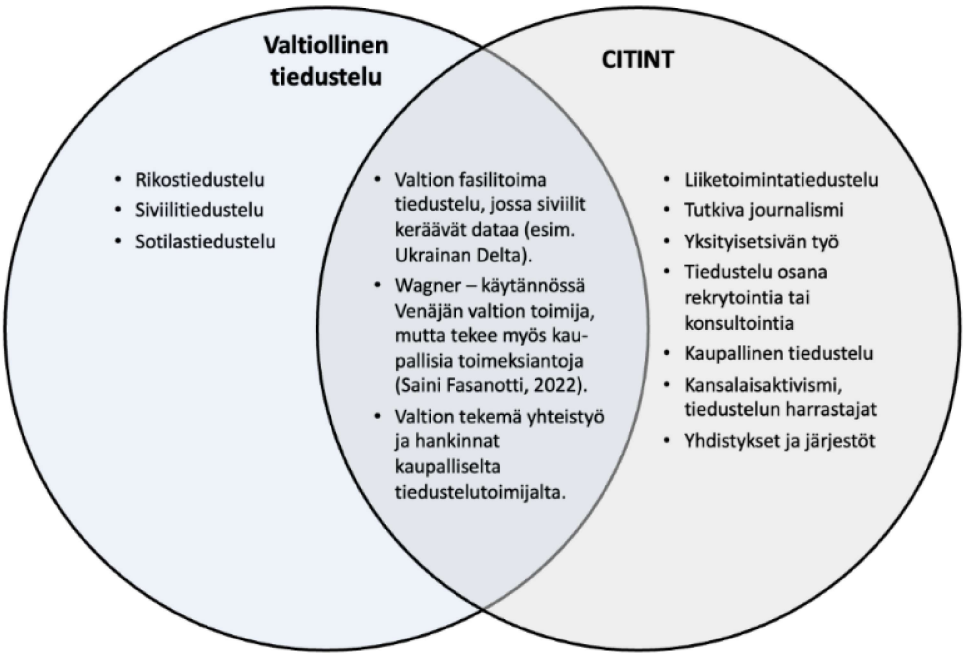
Käsite CITINT määrittyy luontevimmin kolmannen perusteen eli toteuttajan yhteiskunnallisen roolin mukaan. Jos CITINT on määritelmällisesti *ei-valtiollisen toimijan toteuttamaa tiedustelua*, se olisi siten rinnakkaiskäsite sotilas-, siviili- ja rikostiedustelulle.

On huomattava, että tiedustelun käsitteistössä on itse asiassa ollut aukko. Kansalaisten, yhdistysten, yritysten ja vapaiden kollektiivien tekemälle tiedustelulle ei ole ollut olemassa vakiintunutta termiä.

2.2 Kansalaistiedustelun ja valtiollisen tiedustelun rajapinnat

Valtiollinen tiedustelu ja CITINT eivät ole toisistaan täysin irrallisia, vaan niillä on yhtymäkohtia. Kuviosta 1 nähdään kuinka valtio voi fasilitoida CITINTia tuottamalla keräysalustan. Lisäksi valtio voi ostaa CITINT-toimijoilta tiedustelun eri vaiheita tai osatoteutuksia eri tarpeisiin (Saini Fasanotti, 2022). Myös valtion vastatiedustelu saattaa hyötyä CITINTistä, kun kansalaiset voivat ilmoittaa esimerkiksi epäilyttävästä toiminnasta, kuten tiedustelulennokki- eli drone-havainnoista (Lapinkangas & Julkunen, 2022).

Kansalaisten raportoimat tiedot ovat saaneet suuren merkityksen nykyisissä konflikteissa, koska kansalaiset voivat tuottaa arvokasta dataa tukemaan esimerkiksi asevoimia, valtiollista tiedustelua ja humanitäärisiä operaatioita (Pešek, 2023). Tavallaan jokainen jaettu valokuva tai video sosiaalisessa mediassa on tiedusteludatan tuottamista, mutta erityisen arvokasta se on konfliktialueilla kalustosta ja operatiivisesta toiminnasta otetuissa kuvissa ja videoissa.



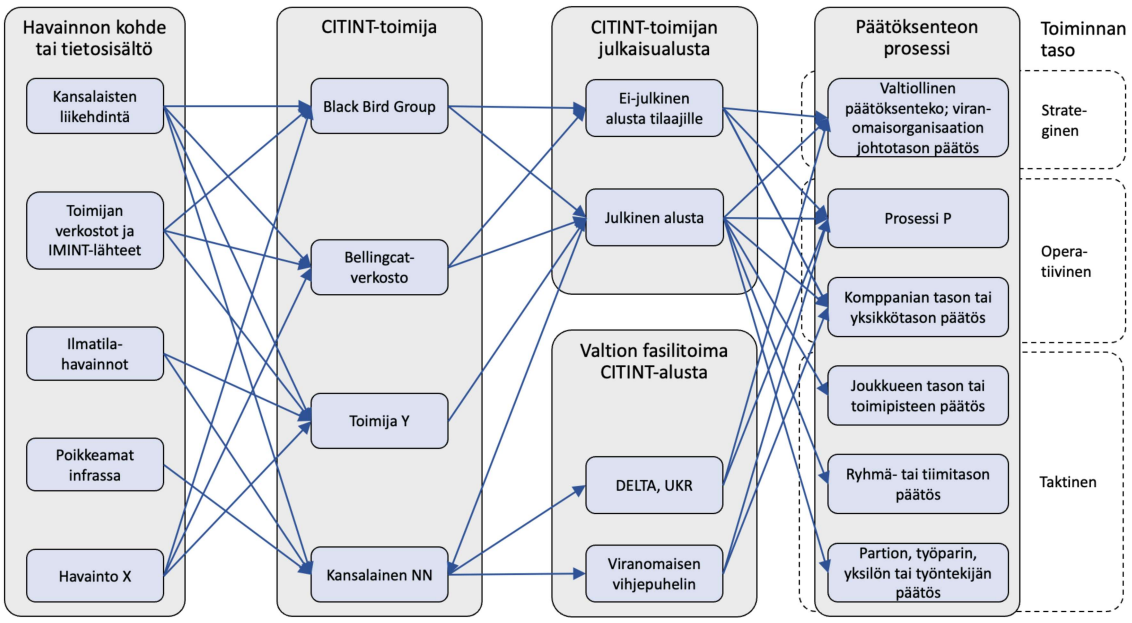
KUVIO 1 Valtiollisen tiedustelun ja CITINTin suhde.

Kansalaistiedustelulla voi olla myös kaupallinen leikkauspinta valtiollisen tiedustelun kanssa. On nimittäin mahdollista, että ansioituneella OSINT-tiedustelun tuottajalla olisi valtiollisia toimeksiantoja jonkin tiedustelutuotteen tuottamiseen tai jakamiseen. Tähän viittasi myös Maanpuolustuskorkeakoulun sotataidon laitoksen johtaja Petteri Kajanmaa, joka kertoi julkisesti MPKK:n tekevän yhteistyötä OSINT-ryhmittymä Black Bird Groupin kanssa (Kajanmaa, 2022).

Emil Kastehelmi kertoo, että Black Bird Group on pitänyt tilannekatsauksia Suomen poliittisille toimijoille. Hänen mukaansa päättäjien ja viranomaisten on helpompi viitata julkisesti sellaiseen tiedustelutietoon, jonka Black Bird Group on kerännyt avoimista lähteistä. Se ei ole salaista eikä turvaluokiteltua, ja lähteeksi voi mainita Black Bird Groupin. Kastehelmi muistuttaa, että organisaatiosta ei voi jakaa ulos salaista tietoa, mutta julkisista lähteistä voi. (Haastattelu 17.10.2023.) Tämän näkökulman vahvistaa myös Martti J. Kari *Ulkopolitiikka*-lehden haastattelussa. Karin mukaan kansalaisten tekemä tiedustelu pystyy tuomaan esiin asioita, joita valtion oma tiedustelu ei voi kertoa, mutta jotka olisi hyvä saada suuren yleisön tietoon. (Vainio, 2021.) Jyrki Isokangas muistuttaa kuitenkin, että tietyissä tilanteissa jo tiedustelutehtävä itsessään voi olla turvaluokiteltu, jonka myötä avoimista lähteistä saadun tiedon analyysi saattaa tuottaa turvaluokiteltua tietoa. Vaikka avoimista lähteistä kerätty tieto on sinänsä toki julkista, siitä voi silti tulla turvaluokiteltua, jos tietoa on analysoitu ja käsitelty. (Isokangas, 2024.)

CITINTin luonteen, roolin ja mahdollisuuksien ymmärtäminen helpottuu, kun ilmiötä kontekstualisoi lähikäsitteillä. Tämän raportin havaintojen mukaan CITINTiin näyttää usein liittyvän avointen lähteiden tiedustelu (OSINT), tilannekuvatuotteet, tilannetietoisuus (engl. *situation awareness*) ja kollektiivinen tietotuotanto. CITINTin kannalta oman merkityksensä ovat saaneet sosiaalisen median työkalut, CITINT-ryhmittymien omat alustat ja työkalut sekä valtiolliset työkalut, joilla mahdollistetaan CITINT-aktiviteettien fasilitointi. Nämä kolme ulottuvuutta kytkeytyvät tiedon keräämiseen, käsittelyyn, analytiikkaan ja jakeluun.

Tässä raportissa merkittävä CITINTin ylätason jaottelu liittyykin nimenomaan yksilöiden omaehtoiseen CITINT-toimintaan, hieman järjestäytyneempään kolmannen sektorin CITINT-toimintaan ja valtiollisesti fasilitoituun CITINT-toimintaan. Kuvio 2 esittää valtiollisen toiminnan ja kansalaistiedustelun rajapinnat ja fasilitointialustat.



KUVIO 2 Valtiollisen tiedustelun ja CITINTin suhde. Kuva esittää miten havainnot, tietosisällöt, toimijat, alustat, päätöksenteon prosessit ja toiminnan tasot kytkeytyvät yhteen.

2.3 Uuden termin tarve

Aiemmin tiedustelutoiminta oli lähinnä valtioiden ja kaupallisten toimijoiden käsissä. Althoffin (2016) mukaan henkilötiedustelua on käytetty läpi ihmiskunnan historian sekä kuningaskuntien ja kansallisvaltioiden turvallisuustarpeisiin ja sotilastiedusteluun että kauppiaitten liiketoiminnallisiin tarpeisiin (Althoff, 2016).

Sittemmin toimijoita on tullut lisää. Yksityiset henkilöt tekevät OSINTia varsin laadukkaalla tasolla (Emil Kastehelmen haastattelu 17.10.2023). Myös tutkivat journalistit käyttävät tiedustelun keinoja (Nelliyullathil, 2020; Scott, 2023).

Uutta termiä tarvitaan, koska sen avulla voidaan määritellä tarkemmin ei-valtiollisten tiedustelutoimijoiden roolit, vastuut ja velvollisuudet. Oletettavissa on, että lainsäädäntöä ei hetkessä saada ajan tasalle CITINT-kentän nopean muutoksen kanssa. Myöskään alan toimijat eivät välttämättä tunnista CITINTiin liittyviä vastuita. Tietävätkö esimerkiksi OSINT-harrastajat, että myös avoimista lähteistä kerätty henkilötieto ja verkostoanalyysi voivat muodostaa GDPR-määräysten (engl. *General Data Protection Regulation*) alaisen henkilörekisterin, jos kerääjänä on yhdistys tai yritys? Entä tunnistavatko CITINTin tekijät eettisen vastuunsa ja hallitsevatko he tietoturvan? Miten toimitaan, jos CITINT-harrastajan keräämä data varastetaan tai se vuotaa ulos? Näihin kysymyksiin pureudutaan tiiviisti raportin luvussa 4.

3 Kansalaistiedustelu CITINT vs. valtion tekemä tiedustelu

Kansalaisten ja yksityisten toimijoiden tekemä tiedustelu eroaa monelta osin valtion tiedustelutoiminnasta. Tässä luvussa käydään läpi oleellisimmat erot rooleissa, toiminnassa ja menettelytavoissa.

3.1 Tiedustelutoiminnan tehtävänanto ja motivaatio

Kansalaisten ja valtioiden tekemän tiedustelun lähtökohdat ovat erilaiset. Valtion tiedusteluorganisaation motiivina on velvoite tiedustelutietojen tuottamiseen valtiotason päätöksenteon tukemiseksi ja valtion turvallisuuden takaamiseksi (Suojelupoliisi, n.d.).

Sen sijaan kansalaisella ei ole täysin samaa näkökulmaa tiedustelutiedon tuottamiseen tai jakamiseen. Kansalaisen motivaationa tiedustelutiedon jakamiseen voi olla pelkästään näkyvyys mediassa ja sosiaalisessa mediassa. Sosiaalisen median sisällön tuottaminen saattaa olla riittävä motivaatio tiedustelutiedon keräämiseen, analysointiin ja julkaisuun.

Yksi CITINT-motivaattoreista on myös kunnianhimo ja halu kehittää kansalaistiedustelua paremmaksi. Emil Kastehelmen mukaan OSINT-ryhmittymä Black Bird Groupin tiedustelumotivaationa ovat olleet median tekemät virheet ja halu tuottaa parempaa tietoa (haastattelu 17.10.2023). Voi myös olettaa, että on olemassa akateemisia motivaattoreita, jolloin tiedustelua tehdään tutkimustyöhön liittyen.

Kansalaistiedustelun motivaatio voi olla myös aatteellinen, jos nähdään, että oma tiedustelutoiminta tukee jollain tapaa omaa ideologiaa. Tiedustelutuote voi olla silloin värittynyt oman ideologian tukemiseksi.

Eräs CITINT-motivaatio on tietenkin yksilön työnkuva: esimerkiksi yksityisetsivien ja tutkivien journalistien työtehtäviin kuuluvat tietyt tiedustelun keinot ja metodit (tutkivan journalistin[2] haastattelu 15.11.2023). Kaupallisella puolella yrityksen tekemän tiedustelun motivaatio on lähinnä päätöksenteon tukeminen.

Lisäksi pitää muistaa, että joidenkin toimijoiden "työnkuva" on lain väärällä puolella. Rikollisjärjestöt käyttävät tiedustelua rikosten suunnitteluun ja kilpailevien liigojen vastavakoiluun, kertoo KRP:n rikosylikomisario Marko Leponen (haastattelu 15.11.2023).

3.2 CITINT-operaatioturvallisuus

Merkittävin ero valtiollisen tiedustelun ja CITINTin välillä näyttää olevan operaatioturvallisuudessa. Marko Leponen kertoo, että rikollisten operaatioturvallisuus on usein heikkoa, ja he esimerkiksi luulevat, ettei prepaid-liittymää voi jäljittää (haastattelu 15.11.2023). Myös Emil Kastehelmi kuvaa, että CITINTin operaatioturvallisuudesta on pidettävä tietoisesti huolta: data pitää säilyttää turvallisesti, eivätkä omat osoitetiedot saa olla julkisia (haastattelu 17.10.2023).

Eroja löytyy myös datan generoijan ja julkaisijan näkökulmasta. Valtiolla on nimittäin tarkat säännökset siitä, mitä julkaistaan ja mitä ei. Sen sijaan moni yksityinen henkilö julkaisee jatkuvasti tiedusteludataa itsestään, läheisistään ja arjestaan. Useat

[2] Kyseinen tutkiva journalisti halusi tietoturvasyistä jättäytyä anonyymiksi, mutta hänet on haastateltu kuvallisen videoyhteyden kanssa. Henkilö on yleisesti tunnustettu alan toimija.

kansalaiset jakavat säännöllisesti kuvia, videoita ja tietoja verkossa, ja tämä aineisto voi olla hyödyksi monelle CITINT-operaattorille.

3.3 Resurssit, osaaminen ja metodit

Valtio kouluttaa tiedustelun ammattilaisia omiin tarpeisiinsa: Maanpuolustuskorkeakoulussa yksi kadettien opintosuunta on tiedustelu, ja myös Puolustusvoimien Tiedustelulaitoksessa toimii Tiedustelukoulu (MPKK, 2019; Puolustusvoimat, n.d.). Sen sijaan tiedustelun avoin akateeminen opiskelu on mahdollistunut vasta syksystä 2019 alkaen Jyväskylän yliopistossa (Vähätalo, 2019). Niinpä voi olettaa, että kansalaistiedustelun tekeminen on pitkälti kokemuksen kautta opittu taito (ks. myös Mitrovich, 2016).

Kansalaisten ja valtion tiedustelutiedon keräys on erilaista useasta näkökulmasta. Valtiolla on salaisia tiedustelulähteitä, joita kansalaisilla ei yleensä samalla tavalla ole. Kansalaisten tiedustelu perustuu pitkälti maksuttomien OSINT-tietojen hyödyntämiseen, joskin myös länsivaltioiden tiedustelutiedot perustuvat nykyään noin 80–90-prosenttisesti OSINT-tietoihin (Ghioni, Taddeo & Floridi, 2023).

Valtioilla on enemmän henkilöstöä ja teknisiä resursseja suorittaa omaa MASINT-, SIGINT-, GEOINT- ja HUMINT-tiedustelua, jonka dataan kansalaisilla on yleensä hyvin rajattu pääsy. Osa karttapalveluiden ja julkisten virastojen satelliittikuvista ja säteilymittaustiedoista jaetaan julkisessa verkossa, jolloin kansalaiset voivat hyödyntää niitä vapaasti. Lisäksi radioamatöörit voivat omalta osin kerätä ja julkaista SIGINT-dataa.

Verkostojen ansiosta kansalaistiedustelijoilla voisi teoriassa olla valtiota suuremmat henkilöstöresurssit tiedusteluun. Valtioilla on rajalliset budjetit, mutta harrastajien yhteistyön tekemiselle ei ole suoraan rajoitteita. Valtion toiminta on kuitenkin paremmin organisoitua ja johdettua, ja yhteinen motivaatio ja tavoitteet ovat selkeämmät. Valtiolla on myös laillisia pakkokeinoja tiedustelutietojen tuottamiseen oman valtion sisällä, esimerkiksi yksityishenkilöiden puheluiden kuuntelu oikeuden päätöksellä. Valtiollisilla toimijoilla on laillinen oikeus vaihtaa keskenään sellaisia tietoja, joihin yksityishenkilöillä tai kaikilla viranomaisillakaan ei ole pääsyä eli tieto on salassapidettävää.

Valtion rooliin kuuluu myös vastatiedustelu, mutta kansalaisten ei yleensä tarvitse käyttää resurssejaan siihen. Sen sijaan kaupallisten yritysten täytyy huomioida mahdollinen liiketoimintavakoilun riski ja käyttää resursseja myös oman toiminnan suojaamiseen kuin mahdollisen kilpailevan tuotteen tai valmistajan tiedusteluun.

Henkilötiedustelua kansalaiset voivat muutenkin tehdä rajatummin, ja käytännössä keinot rajoittuvat yleensä kasvokkain ja verkon yli kommunikointiin. Silti verkon yli kommunikoinnissa voi hyvillä verkostoilla saada tiedustelutietoa, jota ei samalla tavalla ole OSINTin keinoin saatavissa. Niinpä HUMINT voi olla yksi merkittävä tiedustelulähde CITINTissä (Kastehelmen haastattelu 17.10.2023). Tietojen paikkansapitävyyden varmistamisessa ja lähteen luotettavuuden arvioinnissa valtioilla on kuitenkin kaikkien tiedustelulähteiden myötä paremmat mahdollisuudet.

Kaupallisten yritysten tekemä tiedustelu lähtee osittain samoista lähtökohdista kuin yksityishenkilöidenkin, koska lainsäädäntö ja tiedustelukeinot ovat hyvin samankaltaiset. Joillain yrityksillä voi olla käytössään merkittäviä tiedustelulähteitä ja -resursseja, toisin kuin yksittäisillä kansalaisilla. Tällaisia tapauksia ovat esimerkiksi Venäjän valtion hyödyntämä yksityisarmeija Wagner, joka periaatteessa on yritys mutta käytännössä valtion käsikassara. Lisäksi yrityksellä voi olla enemmän resursseja ostaa OSINT-

tiedustelutietoja kuin yksityisellä kansalaisella, ja näin yrityksellä on parempi pääsy maksullisiin tietoihin.

3.4 Valtioiden rajat ylittävä CITINT ja valtiollinen tiedustelu

Sekä valtio että kansalaiset tekevät myös valtioiden rajat ylittävää tiedustelua. Tämänkin suhteen CITINTilla ja valtiollisella tiedustelulla on eroja metodeissa, resursseissa ja lainsäädännössä. Valtioilla on eri maissa lähetystöjä, joissa tehdään laillista tiedustelua kohdemaasta ja sen tilanteesta. Tällöin valtion keräämät tiedustelutiedot ovat globaalimpia ja keskitetymmin koottuja kuin kansalaisilla. Lisäksi valtiolla voi olla käytössään vieraasta maasta paikallisesti värvättyjä agentteja, joilta saa kohdevaltiosta tiedusteludataa (Isokangas, 2023c). Valtiot tekevät keskenään tiedusteluyhteistyötä monella eri tasolla (Isokangas, 2023d). Viranomaiset tekevät valtioiden rajat ylittävää rikostiedustelua sekä siviili- ja sotilastiedustelua, joka kohdistuu kansallista turvallisuutta vakavasti uhkaavaan toimintaan (Hakonen, 2020).

Myös CITINT-toimijat voivat kerätä globaaleja tietoja OSINT-menetelmin, joskin tiedon keräämisen lähtöasetelmat vaihtelevat merkittävästi. Kansainvälinen CITINTiä tekevä yritys voi saada toimipaikkojensa ja alihankkijoidensa ansiosta tietoja enemmän ja helpommin kuin yksittäinen kansalaistoimija tai -ryhmittymä. Lisäksi kansainvälisillä rikollisjärjestöillä voi olla käytössään soluttautujia ja tietolähteitä viranomaisorganisaatiossa tai infrastruktuuria hallinnoivassa yrityksessä (Mäntysalo & Pietarinen, 2023 sekä SVT, 2023).

Useiden valtioiden lainsäädäntö ja kansainväliset säännökset rajoittavat värväämistä, kieltämällä muun muassa pakottamisen ja kiristämisen. Edelleen ulkomailla toimiessa täytyy huomioida muiden valtioiden erilaiset säädökset ja ihmisoikeustilanteet, joten kansalainen voi myös varomattomalla toiminnalla saattaa itsensä vaaraan kyselemällä tietoja kohdemaan kansalaisilta tai muutoin dokumentoimalla tai tallentamalla tietoja ulkomailla. Kohdemaan kulttuuri, kieli ja toimintaympäristö pitää tuntea erittäin hyvin, jos tiedustelua kohdennetaan vieraisiin valtioihin tai niiden toimijoihin ja organisaatioihin.

Ulkomailla toimiessa on huomioitava myös joidenkin valtioiden eristetty ja valvottu internet ja media. Esimerkiksi Kiinassa tapahtumia valvotaan tarkasti niin internetissä kuin kaupungillakin (Lyytikkä & Hallamaa, 2018). Tällöin internetistä ja mediasta kerätty tieto on todennäköisesti vääristeltyä eikä kerro luotettavaa tietoa toiminnasta. Haasteeksi voi nousta se, että todellista tietoa ei ole CITINT toimijoiden saatavilla puuttuvien tiedusteluresurssien vuoksi, kun taas viranomaisilla on enemmän keinoja tiedustella todellisia tapahtumia kansalaisille kerrotun sijasta.

4 CITINT ja lainsäädäntö

Suomen tiedustelulainsäädäntö koskee viranomaisia. Lain perusteella tiedustelu on sallittua viranomaistoiminnassa tietyin edellytyksin ja tietyissä tapauksissa. Sen sijaan kansalaisen tekemään tiedusteluun, joko organisoidun verkoston tai yksittäisen toimijan näkökulmasta, ei ole olemassa erillistä lainsäädäntöä tai yksittäistä ohjaavaa lakia. Jukka Mäki-Kuhna onkin todennut, että mitä enemmän kansalainen kerää tiedustelutietoa, sitä suurempi vaara on joutua juridisiin vaikeuksiin (Mäki-Kuhna, 2023).

Tässä osiossa esitetyt lait ovat sellaisia, jotka on hyvä huomioida CITINTissä. Lista ei ole täydellinen, vaan tässä tarkastellaan tyypillisimpiä tilanteita, joissa oletettavasti täytyy huomioida myös juridinen näkökulma. Tässä luvussa pysytellään pääasiassa Suomen lainsäädännön sisällössä, mutta lukijaa pyydetään huomioimaan myös kansainvälisesti vaikuttavat EU:n ihmisoikeussopimukset (EU, n.d.) sekä esimerkiksi Geneven sopimus siviilihenkilöiden suojelemisesta sodan aikana (Ulkoasiainministeriö, 2015).

4.1 Perustuslaki ja tietosuojalaki

Suomen perustuslain (791/1999) 2. luvussa säädetään perusoikeuksista, jotka koskevat jokaista kansalaista tai maassa laillisesti oleskelevaa. Perusoikeuksia ovat muun muassa yhdenvertaisuus (6 §), liikkumisvapaus (9 §), yksityiselämän suoja (10 §), sananvapaus ja julkisuus (12 §) sekä omaisuuden suoja (15 §). Lista ei ole kattava, vaan tähän on poimittu tiedustelun kannalta olennaisimmat. Perustuslain säännöksistä voi poiketa ainoastaan muussa lainsäädännössä määritellyllä tavalla, mutta muutoin kaikessa toiminnassa täytyy huomioida tämän lain säännökset. Lisäksi on hyvä huomioida myös perustuslain 8 § rikosoikeudellinen laillisuusperiaate: ketään ei saa pitää syyllisenä rikokseen, jota ei tekohetkellä ole laissa säädetty rangaistavaksi (perustuslaki 1999). Pykälä kytkeytyy esitutkintalain (805/2011) 4. luvun 2 §:n syyttömyysolettamaan. Jos henkilön osuutta tapahtumien kulkuun vasta tutkitaan, hänestä ei voi käyttää termiä rikollinen, vaan hän on aina epäilty. Siinä vaiheessa, kun tekijä on Suomen lainsäädännön mukaan tuomittu oikeudessa, häneen voidaan viitata rikollisena.

Jo tiedustelutiedon keräystä suunnitellessa täytyy huomioida juridiikan näkökulmasta, syntyykö keräyksen yhteydessä mahdollisesti tallennettuja henkilötietoja sisältäviä dokumentteja (teksti, ääni tai kuva). Niiden säilyttämiseen on omat vaatimuksensa lainsäädännössä. Tietosuojalaki (1050/2018) säätää henkilötietojen keräyksestä, säilytyksestä ja käsittelystä, ja sen tarkoituksena on turvata tiedon luotettavuus, eheys ja saatavuus. Lain taustalla on koko EU:n kattava tietosuoja-asetus GDPR. Tietoa on kerättävä vain tarpeellisiin tarkoituksiin; sitä on säilytettävä ja käsiteltävä siten, ettei kukaan ulkopuolinen pääse tietoon käsiksi muuttamaan tai lukemaan sitä, ja lisäksi tallennettu tieto on luovutettava rekisteröidylle hänen pyynnöstään. (Tietosuojalaki, 2018.)

Tietosuojalaki painottuu organisaatioiden ja yritysten keräämään tietoon enemmän kuin yksityisen kansalaisen keräämään tietoon. Yksityinen henkilö saa sinänsä kerätä tietoa vapaammin omiin tarkoituksiin eikä siitä tarvitse tehdä rekisteriselostetta, mutta tällöin korostuu ennen kaikkea tiedon käyttötarkoitus ja julkaisu. Yksityisen tiedon keräystä ja tiedon levitettävyyttä ohjaa muun muassa perustuslain pykälä sananvapaudesta (perustuslaki 1999, 12 §). Tiedon levitettävyyteen vaikuttavat rikoslaissa määritetyt rangaistukset yksityisen tai salassapidettävän tiedon levittämisestä, joten täysin vapaata yksityisen henkilön tiedon ja mielipiteen levittäminen sananvapauden nimissä ei ole. Rajoittavia säännöksiä käydään läpi tarkemmin seuraavassa alaluvussa.

4.2 Järjestyslaki ja rikoslaki

Todennäköisesti tiedustelutiedon kerääjä törmää siihen kysymykseen, saako hän ottaa kuvia tai videoita ja kuunnella tai tallentaa ääntä. Lähtökohtaisesti järjestyslain (612/2003) mukaisissa yleisissä paikoissa kuvaaminen on sallittua. Julkisia paikkoja ovat alueet, jotka ovat yleisön käytettävissä, muun muassa tiet, puistot, torit, uimarannat ja

joukkoliikenteen kulkuneuvot. Lisäksi julkisiin paikkoihin luetaan ne rakennukset, jotka ovat yleisön käytettävissä jonkin tilaisuuden aikana tai liikkeen aukiolon puitteissa. Näitä ovat virastot, toimistot, liikenneasemien ja kauppakeskusten yleiset alueet sekä ravintolat. (Järjestyslaki 2003 2 §.) Näissä tiloissa kuvaamista ei voi kieltää, jos toiminta ei ole muutoin häiritsevää. Sen sijaan julkisrauhan ja kotirauhan suojaamilla alueilla kuvaamiseen tarvitsee alueen omistajan tai toiminnanharjoittajan luvan. Julkisrauhan suojaamia paikkoja ovat yleisten paikkojen yleisöltä suljetut osat sekä osat ja paikat, rakennukset ja alueet, joihin on rajoitettu pääsy. (Rikoslaki 39/1889.)

Tallennetun dokumentin julkaisemisessa on enemmän huomioitavia seikkoja myös yksityisellä tiedustelijalla. Jos tallennettu dokumentti sisältää yksityiselämää koskevaa tietoa tai kyseinen dokumentti loukkaa dokumentissa tunnistettavasti esiintyvän henkilön kunniaa, voi julkaisussa syyllistyä rikokseen. Yksittäinen kansalainen voi esimerkiksi tallentaa kaikki omat puhelut sekä kuvata julkisilla paikoilla videota ja kuvaa, ja osittain tätä voi tehdä jopa yksityisellä alueella, kun edellytykset täyttyvät. Silti sillä on merkitystä, miten tallennetta käyttää: asettaako aineiston muiden saataville tallennetun henkilön yksilöä loukkaavalla tavalla vai käyttääkö sitä esimerkiksi oikeudessa todisteena, jolloin sillä on rajatumpi näkymä. Jälkimmäinen on sallittua, sillä oikeudessa voi esittää todisteena yksityiselämää sisältävän dokumentin.

Rikoslaissa (39/1889) on lueteltu kaikki rikokset, joista voidaan tuomita, jos lakia ei noudata. Rikoslain (39/1889) 24. luvussa säädetään yksityisyyden, rauhan ja kunnian loukkaamisesta. Nämä säännökset suojaavat yksilöä ja osittain organisaatioita hyvin vahvasti yhdessä muun lainsäädännön kanssa, joten tiedustelua tekevä kansalainen joutuu ensiksi miettimään tämän luvun säännöksiä tietoa hankkiessaan. Luvun säännökset sisältävät muun muassa kotirauhan rikkomisen (1 §), julkisrauhan rikkomisen (3 §), salakatselun (6 §), salakuuntelun (5 §), edellä mainittujen valmistelun (7 §), kunnianloukkauksen (9 §), yksityisen tiedon levittämisen (8 §) ja muut vastaavat toimet. Vapauteen kohdistuvia rikoksia käsittelevän 25. luvun 7a §:ssä säädetään vainoamisesta, johon voi syyllistyä seurantaa tekemällä. Jos taas kansalaistiedustelija vaatii jotakuta luovuttamaan jotain tietoa vastoin tämän tahtoa, niin kyseessä on 8 §:n pakottaminen. Rikoslaki kieltää myös kiristyksen 31. luvun 3 §:ssä.

Toinen merkittävä rikoslain osa on 38. luku, joka käsittelee tieto- ja viestintärikoksia. Siinä säädetään muun muassa salassapidosta (1 §), viestintäsalaisuuden loukkauksesta (3 §), tietoliikenneverkon häirinnästä (5 §), tietojärjestelmän häirinnästä (7 §), tietomurrosta (8 §), suojauksen purkujärjestelmärikoksesta (8b §), tietosuojarikoksesta (9 §) sekä identiteettivarkauksista (9a §). (Rikoslaki 39/1889.) Nämä säännökset kaventavat Suomessa kansalaisten tiedustelua verrattuna viranomaisia velvoittavaan tiedustelulainsäädäntöön. Nämä säännökset koskevat myös oikeushenkilöä eli järjestäytyneitä organisaatioita.

Rikoslain (39/1889) 15. luvun 10 §:ssä taas on jokaisen kansalaisen velvoite antaa ennakkovaroitus viranomaisille tai sille, jota rikos uhkaa, tietyistä vakavista rikoksista, jos saa tietoonsa sellaisen tai sen valmistelun. Tämä ei koske tilannetta, jossa rikoksen valmistelija sattuu olemaan lähisukulainen.

Liiketoimintatiedustelun kannalta rikoslain (39/1889) 30. luvussa säädetään elinkeinorikoksista, joista tiedustelijan kannalta on merkittävin 2 § kilpailumenettelyrikos ja 4 § yritysvakoilu. Lisäksi samassa 30. luvussa on säännökset yrityssalaisuuksista (5 §) ja niiden väärinkäytöstä (6 §). (Rikoslaki 39/1889.)

Rikoslaissa on myös omat säännökset Suomen valtiota vastaan tehtyihin rikoksiin, ja nämä ovat yleisen syytteen alaisia rikoksia. Useissa muissakin rikoslain pykälissä, jotka on mainittu jo aiemmin tässä luvussa, syyttäjällä on oikeus nostaa syyte yleisen edun sitä vaatiessa, vaikka pääasiassa muutoin rikokset ovat asianomistajarikoksia.

Suomen valtiota vastaan tehdyistä rikoksista erityisesti maanpetosrikokset ovat tiedustelun näkökulmasta merkittäviä. Nämä esitetään rikoslain luvussa 12. ja erityisesti sen 9 §:ssä laiton tiedustelu.

> Luvaton tiedustelutoiminta: Joka vierasta valtiota vahingoittaakseen tai toista vierasta valtiota hyödyttääkseen hankkii tietoja vieraan valtion maanpuolustuksesta, turvallisuudesta tai niihin välittömästi vaikuttavista seikoista ja siten aiheuttaa vahinkoa tai vaaraa Suomen ulkomaansuhteille, on tuomittava luvattomasta tiedustelutoiminnasta vankeuteen vähintään neljäksi kuukaudeksi ja enintään kuudeksi vuodeksi. Yritys on rangaistava. (Rikoslaki 12. luku 9 §.)

Tämä asettaa rajoituksia tiedon julkaisemiseen. Jos pykälän mukaista tietoa nousee julkisuuteen siten, että Suomen suhteet heikkenevät kansainvälisesti arvioituna, on tekijä tuomittava rangaistukseen. Maanpetososio käsittää myös kaikki Suomea vastaan tai Suomen asemaan heikentävästi vaikuttavat kansainväliseksi katsotut rikokset. Lisäksi luvussa 13 käsitellään valtiopetosrikoksia. (Rikoslaki 39/1889.)

4.3 Yhteenveto kansalaistiedustelua koskevasta lainsäädännöstä

Kun toimii vastoin lakia, on sillä myös seuraamukset. KRP aloitti tutkinnan eräästä turvallisuussalaisuuden paljastamisesta huhtikuussa 2023 (poliisi, 2023). Tämän tyyliset rikokset Suomessa ovat harvinaisia, ja tapaus sai valtakunnan medioissa paljon uutistilaa paljastuessaan; olivathan epäillyt myös ehdolla eduskuntavaaleissa. Tarkalleen ei ole paljastettu, mistä rikosepäily juontuu, mutta epäillyt ovat pitäneet nettisivustollaan ja Youtube-kanavallaan esillä niin sanottua tunnelisotateoriaa, ja tämän ohessa he ovat pitäneet karttakuvaa Suomen tunneleista. Nyt jo poistetuista videoista voi todeta, että epäillyt ovat tunneleita kartoittaessaan menneet alueille, joissa liikkuminen on lain mukaan luvanvaraista (Vapa, 2023).

Tapaus on hyvä esimerkki kansalaisten suorittamasta epäonnistuneesta tiedustelusta: jos ei tunne lainsäädäntöä, saattaa itse tulla syytetyksi. Yksityisen henkilön keräämä tieto ei sinänsä ole välttämättä rikollista, mutta se miten sen kerää, miten sen julkaisee ja kenelle, on erityisen huomion arvoista. Tämä tapaus myös osoittaa oman toiminnan suojaamisen tärkeyden.

Jos CITINTin määritelmään lasketaan kuuluvan kaikki ei-valtiollinen tiedustelutoiminta, niin riippuen toiminnan organisoitumistavasta ja toiminnasta, huomioitavien lakien ja ohjeiden määrä vain kasvaa. Esimerkiksi journalisteilla ja medialla on omat lakinsa sekä eettiset ohjeet, ja yksityisetsivän tulee taas huomioida yksityistä turvallisuuspalveluista annetun lain säädökset.

5 Esimerkkejä CITINT-toimijoista ja työkaluista

Suomessa toimii muutamia CITINT-ryhmiä, -organisaatioita ja -yrityksiä. Tässä raportissa ei luonnollisesti voida listata kaikkia alan toimijoita, vaan pikemminkin kyseessä on

katsaus suomalaiseen CITINT-kenttään ja niihin organisaatioihin, joiden aktiviteetit voidaan lukea CITINTin alle. Mukana on myös kansainvälisiä esimerkkejä.

Lisäksi luvussa esitellään kaksi työkalua, joita CITINT-toimijat voivat hyödyntää. Esimerkeiksi valikoituivat Ukrainan Delta ja julkinen Blackbird-työkalu, sillä ne edustavat CITINTin eri paradigmoja (bottom-up ja top-down).

5.1 CITINT-toimijoita

5.1.1 CITINT-ryhmiä

Black Bird Group lienee Suomen tunnetuin CITINT-ryhmä. Se sai alkunsa hieman ennen Ukrainan sodan alkua, kun OSINT-harrastajat Eerik Matero, John Helin ja Emil Kastehelmi päättivät varautua rintamalinjojen seurantaan helmikuussa 2022. Kastehelmen mukaan ryhmän tunnettuus kasvoi nopeasti. Black Bird Group toimi yli vuoden ilman nimeä, kunnes ulkomaiset toimijat pyysivät ryhmää keksimään itselleen nimen. Black Bird Group on sittemmin rekisteröitynyt yhdistykseksi, ja tavoitteena on jatkossakin tuottaa kaupallisia tiedustelutuotteita myyntiin. (Kastehelmen haastattelu 17.10.2023.)

Kastehelmi olettaa, että Suomessa on muitakin vastaavia ryhmittymiä, mutta hän ei osannut suoraan nimetä muita. Ainakin vapaan kansainvälisen OSINT-verkoston Bellingcatin aktiiveissa on ollut mukana suomalainen Veli-Pekka Kivimäki (Higgins, 2021, esipuhe). Kansainvälisiä CITINT-ryhmiä on Bellingcatin lisäksi muun muassa InformNapalm ja OpenSky Network. Lisäksi monet kansalaisjärjestöt tarvitsevat tiedustelutietoa avustusoperaatioihinsa. (Vainio, 2021.)

5.1.2 Tutkivan journalismin yhdistys ry

Tutkivan journalismin yhdistys ry on perustettu 24.11.1992 (Tutkivan journalismin yhdistys, 2011). Tutkivassa journalismissa tiedonhankintaan ja -analyysiin käytetään sekä OSINT- että HUMINT-tekniikoita (Nelliyullathil, 2020; Scott, 2023). Lisäksi käytössä on taloudellisen tiedustelun metodeja eli FININT-analyysia (Scott, 2023).

Lähdeaineistoon saatiin mukaan anonyymiksi jättäytyvän tutkivan journalistin haastattelu. Haastateltava vahvisti, että edellä mainitut OSINT, HUMINT ja FININT ovat käytössä. Lisäksi hän kuvasi massiivista työtä, jota tehdään tietoaineistojen kanssa. Usein tietovuodot sisältävät suuren määrän raakadataa, jossa voi olla useiden tietokoneiden, virtuaalikoneiden ja palvelimien sisältämä data. Tämän perkaaminen vaatii tekijältään ict-osaamista, jotta raakadata saadaan käsiteltyä käyttökelpoiseen muotoon. (Tutkivan journalistin haastattelu 15.11.2023.) Työvaihe on siis täysin sama kuin valtiollisessakin tiedustelussa, kun raakadataa käsitellään informaatioksi (Isokangas, 2023b).

Haastateltava kertoi, että tutkivan journalistin työssä tärkeä tietolähde on vakioinformantti eli "syväkurkku", jonka kanssa saatetaan pitää yhteyttä vuosien ajan. Haastateltava korosti, että kyseessä ei ole ystävyyssuhde, vaan ammatillinen luottamussuhde. Käytännössä syväkurkun käyttö vertautuu valtiollisen tiedustelun HUMINT-agenttiin, joka värvätään esimerkiksi toisesta valtiosta (Isokangas, 2023c). Haastateltu kertoi, että alalla tällaista lähdettä pidetään timantin arvoisena, ja siksi tutkiva journalisti saattaa pitää puolen vuoden välein yhteyttä lähteeseen ja kysyä tältä kuulumisia (haastattelu 15.11.2023).

Tutkivan journalismin alalla pidetään usein kansainvälisiä konferensseja, joissa kouluttaudutaan alan metodeihin, juttuprosesseihin ja eri maiden lainsäädäntöihin.

Tiedustelun tekniikoita siis kehitetään ja jaetaan kollegoille säännöllisesti, jolloin tiedusteluosaaminen pysyy vahvana. (Tutkivan journalistin haastattelu 15.11.2023; GIJN, n.d.; Tutkivan journalismin yhdistys, 2023.)

5.1.3 Suomen yksityisetsivä- ja lakitoimistoliitto ry

Suomen Yksityisetsivä- ja Lakitoimistoliitto ry on perustettu vuonna 1972 (SYL, n.d.-a). Alalla pyritään hankkimaan, käsittelemään ja säilyttämään tietoa vastuullisesti, sillä liiton eettisissä säännöissä mainitaan ohjenuorina muun muassa tietoturva, tiedon vastuullinen säilytys, lain noudattaminen, puolueettomuus ja luottamuksellisuus (SYL, n.d.-b).

Oikeustieteen tohtori Jyri Paasonen käy blogissaan läpi yksityisetsivien tietolähteitä. Näitä ovat julkiset lähteet (OSINT) ja toimeksiantajalta saatu tieto (HUMINT). Lisäksi Paasonen mainitsee esimerkiksi julkisella paikalla tapahtuvan tarkkailun ja kilpailevan yrityksen asiakkaana esiintymisen, jotka edustavat yhtä aikaa sekä OSINT- että HUMINT-toimintaa. (Paasonen, 2023.)

5.1.4 Muut kaupalliset CITINT-toimijat

Kaupallisia CITINT-toimijoita on lukuisia. Osalla tiedustelu on päätoimialana ja osalla se on vain yksi palveluiden osa-alue vaikkapa konsultoinnissa tai rekrytoinnissa.

Esimerkiksi Iceye Oy on kaupallinen tiedusteluyritys, joka tuottaa satelliittikuvaa, analyyseja ja raportteja (Iceye, n.d.). Voi siis perustellusti todeta, että Iceyen päätoimialana on tiedustelu, vaikka sellaista toimialaluokkaa Tilastokeskus ei tunnekaan (Tilastokeskus, n.d.). Yrityshakemisto Finderin mukaan Iceyen päätoimiala on 71121 Yhdyskuntasuunnittelu (Finder, n.d.). Toki toinen mahdollinen tiedusteluyrityksen päätoimiala voisi olla 63990 Muualla luokittelematon tietopalvelutoiminta (Tilastokeskus, n.d.). Tiedustelutietoa tarjoavat myös monet muut kaupalliset yritykset kuten Clock & Cloud Intelligence ja Cyberwatch Finland. Clock & Cloud on erikoistunut geopolitiikkaan ja Cyberwatch digitaaliseen turvallisuuteen (Clock & Cloud, n.d. ; Cyberwatch Finland, n.d.).

Monet konsultti- ja suorahakuyritykset käyttävät tiedustelua osana palveluvalikoimaansa. Esimerkiksi rekrytointiyritys Inhunt kertoo sivuillaan, että suorahakuprosessin vaiheita ovat muun muassa sopivan henkilön löytäminen, mukaan saaminen, valinta, soveltuvuusarvio, päätöksen auttaminen ja seuranta (Inhunt, n.d.). Malli on siis hyvin lähellä HUMINTin värväysmetodia, jossa ensin maalitetaan sopiva kohde, tutkitaan tämän taustat, luodaan kontakti, kehitetään kohdetta, värvätään hänet agentiksi ja lopuksi siirretään agentti käsittelyvaiheeseen (Isokangas, 2023c).

Myös tietoturvayritysten ja muiden turvallisuusalan toimijoiden palveluvalikoimaan kuuluu haavoittuvuuksien haku myös OSINT-tekniikoilla. Suomessa muun muassa tietoturvayritykset 2NS ja Mint Security tarjoavat OSINT-konsultaatiota, jossa avointen lähteiden kautta selvitetään asiakasyrityksen haavoittuvuuksia (2NS, n.d.; Mint Security, n.d.). Kansainvälisesti CITINT-palveluita myyvät muun muassa ranskalaiset Digimind ja KB Crawl, brittiläiset Oxford Analytica ja Janes, yhdysvaltalaiset Stratfor, Recorded Future, McKinsey, Verint Systems, DigitalGlobe ja Palantir Technologies sekä Puolasta kotoisin oleva Bearstone (Vainio, 2021).

Kaupallinen toiminta on todennäköisesti kasvamassa, koska tiedon tarve kasvaa jatkuvasti. Markkinatutkimusyhtiö Market Research Futuren mukaan OSINT-liiketoiminnan kysynnän kasvuvauhti on 20 prosenttia vuodessa (n.d.).

5.1.5 Rikolliset CITINT-toimijat

Kaikki CITINT-toimijat eivät kulje lain oikealla puolella. Suomessakin toimii järjestöjä, jotka tekevät rikoksiin liittyvää tiedustelua, tiedonhankintaa ja vakoilua. KRP:n rikosylikomisario Marko Leponen kertoo, että Suomessa on yksittäisiä rikollisia ja rikollisryhmiä, jotka tekevät puoliammattimaista tiedustelua. Leponen muistuttaa, että rikollisia eivät estä lainsäädännölliset rajoitteet, joten heidän keinovalikoimaansa kuuluvat muun muassa väkivallalla uhkailu, laittomat tekniset tiedustelulaitteet, tietomurrot ja tietomurroilla saadun tiedon ostaminen. Toki myös yksittäinen ihminen voi sortua käyttämään laitonta tiedustelulaitetta kuten tutkanpaljastinta, vaikkei olisikaan taparikollinen. Leposen mukaan rikollisryhmien heikko kohta on usein operaatioturvallisuus, minkä ansiosta poliisi pääsee toimintaan kiinni. (Leposen haastattelu 15.11.2023.)

Myös Ylen uutisartikkelista voi päätellä, että Turussa vuonna 2002 tehty arvokuljetusryöstö on aikanaan vaatinut tiedustelua. Ryöstöä yrittäneillä on ollut hallussaan paitsi arvokuljetuksen aikataulu, myös pakettiauton sisäpiirustukset. Ryöstö epäonnistui, koska pakettiauto oli eri mallia kuin piirustuksissa. (Collan, 2020.)

5.2 CITINT-alustoja ja työkaluja

Tässä alaluvussa tarkastellaan kahta CITINT-toiminnassa käytettyä työkalua: Delta-työkalu on valtiollisen CITINT-fasilitoinnin keino, ja Blackbird[3] on avoin hakutyökalu.

5.2.1 Ukrainan Delta

Ukrainan puolustusvoimilla on käytössään tilannekuvatyökalu[4] ja -alusta, joka kantaa nimeä Delta (kuva 1). Delta mahdollistaa integratiivisen tilannekuvan tuoton ja ylläpidon, jossa voidaan yhdistää muun muassa ilmakuvauksella, satelliiteilla, kameroilla, tutkilla ja chatboteilla tuotettua aineistoa (Lozovenko, 2023). Järjestelmä on tosiaikainen, ja paikkatietoa hyödyntävä karttatoiminnallisuus on sen keskeisiä ominaisuuksia. Lisäksi Deltan kehitystyössä on pyritty käyttäjän (engl. *client*) alusta-agnostisuuteen, eli sen tulisi olla käytettävissä tietokoneilla, älypuhelimilla ja tableteilla.

Deltaa on ollut kehittämässä Puolustusteknologioiden innovaatio- ja kehittämiskeskus, joka on osa Ukrainan puolustusministeriötä (Militarnyi, 2023). Deltan käyttöperiaatteisiin on ainakin Borgerin (2022) mukaan lukeutunut OSINT-aineistoa järjestelmään syöttävä vähemmän sotilaallinen osasto. Deltan kehityksessä on huomioitu NATO-yhteensopivuus ja -integroitavuus esimerkiksi Link 16 -järjestelmään, joka on useissa NATO-maissa käytössä oleva taktinen datalinkkijärjestelmä (Fornusek, 2023). Työkalussa on pyritty ajattelemaan liittoutuneiden doktriineja modernisti, ja siinä onkin huomioitu useassa ulottuvuudessa toimiminen (engl. *multi-domain operations*) (Militarnyi, 2022).

[3] Blackbird-työkalua ei saa sekoittaa suomalaiseen Black Bird Group -CITINT-ryhmään.

[4] Endsley (1995) purkaa tilannetietoisuuden (engl. *situational awareness*) käsitteen perseptioon, komprehensioon ja projektioon. Nämä tarkoittavat tilanteen havainnointia, ymmärrystä ja arvioita tilanteen kehityssuunnista. Tilannekuvalla tarkoitetaan tässä tutkielmassa tapaa integroida, esittää ja jakaa tilannetietoisuutta. Tilannekuvatyökaluilla tarkoitetaan sellaisia työkaluja, palveluita, alustoja ja ohjelmistoja, joilla tilannekuvatuotteita ja tilannetietoisuuden representaatioita tuotetaan esimerkiksi aikajanana tai karttana.

KUVA 1 Delta-järjestelmä (Borger, 2022).

5.2.2 Blackbird-työkalu

Blackbird-työkalulla voi etsiä käyttäjiä nimimerkillä internetin eri palveluista, mukaan lukien useat sosiaalisen median palvelut, suoratoistopalvelut, pelialustat ja -kaupat sekä blogi- ja repositorioalustat. Dokumentaation mukaan työkalu kohdistaa haun 581 eri palveluun. Blackbird-työkalu on ladattavissa GitHub-palvelusta p1ngul1n0-tilin repositoriosta omassa ympäristössä suoritettavaksi, mutta kokeiltaessa 2.11.2023 palvelu oli käytettävissä myös selaimella[5] . Työkalua voi käyttää komentoriviltä (CLI), mutta repositorion paketti sisältää myös web-palvelimen, jonka avulla työkalua voi käyttää selaimella.

KUVA 2 Blackbird-työkalun logo sekä Blackbirdin CLI-käyttöliittymä (Soeiro, 2022).

6 Johtopäätökset

Vaikka CITINTissä on tunnistettu monia vahvuuksia ja mahdollisuuksia, tässä raportissa tunnistettiin myös siihen liittyviä haasteita ja heikkouksia. CITINTillä tuotetun tiedon tuominen esimerkiksi valtiollisen tai sotilaallisen tilannekuvan ja päätöksenteon

[5] https://blackbird-osint.herokuapp.com/

järjestelmiin on järjestelmätasolla monimutkainen kokonaisuus, jossa liikutaan useiden ei-yhteismitallisten ja strukturoimattomien datakokonaisuuksien välillä. On teknisesti ja arkkitehtonisesti haastavaa luoda vakaat ja koherentit integraatiot järjestelmien välille, vaikka kolmannen osapuolen rajapintoihin voisikin joissain tapauksissa tukeutua.

Lisäksi jos tuotteiden jakelu tai käsittely on CITINT-toimijan puolella riippuvainen kolmannen osapuolen palveluista, voidaan törmätä muun muassa saatavuuden (engl. *availability*) ongelmiin ja tietenkin tiedon luottamuksellisuuden vaarantumiseen. Myös eri CITINT-organisaatioiden ja työkalujen välillä tunnistettu prosessien ja struktuurien heterogeenisyys monimutkaistaa integraatioita. Lisäksi tiedon käyttäjän on luotava mekanismit hyödynnettävän tiedon luotettavuuden arvioinnille ja kiinnittää erityistä huomiota tiedon validointiin ja verifiointiin, sillä CITINT voi olla altis vaikuttamiselle. Suomen kontekstissa oman haasteensa tuovat tiedon salassapitoon ja luokitteluun liittyvät mekanismit, joten on pohdittava, miten varmistutaan tiedon oikeanlaisesta ja oikea-aikaisesta turvallisuusluokittelusta.

CITINTin prosessien ja organisaatioiden nopea kehitys asettaa erityisiä vaatimuksia lainsäädäntötyölle ja kansainvälisten sopimusten sisältämille määritelmille. Tulkitaanko CITINT-toimija esimerkiksi Geneven sopimuksen siviilihenkilöitä koskevan osion mukaan 4. artiklan mukaiseksi suojeltavaksi henkilöksi? Vai sovelletaanko häneen 5. artiklassa määriteltyjä poikkeuksia, jossa ”[– –] selkkauksen osapuolella on pätevää aihetta epäillä, että tietty tämän sopimuksen suojelema henkilö ryhtyy valtion turvallisuutta vaarantavaan toimintaan, tai jos on selvitetty hänen itse teossa siihen ryhtyneen [– –]” (Ulkoasiainministeriö, 2015). Asian pohdinta on erityisen ajankohtaista, sillä tiettyjen tulkintojen mukaan esimerkiksi suomalaisen yrityksen Iceyen voidaan ajatella olevan osapuolena Venäjän Ukrainaan kohdistamassa hyökkäyssodassa, sillä se mahdollistaa merkittävän suorituskyvyn Ukrainalle. Siten Venäjä voisi oikeutetusti kohdistaa vaikuttamista yrityksen satelliitteihin. (Ks. esim. Militarnyi, 2023; Court, 2023; Nasu, 2022; Nasu 6.9.2022.)

Tässä raportissa on tunnistettu myös useita CITINTin mahdollisuuksia ja vahvuuksia. CITINT voi parhaimmillaan mahdollistaa erittäin nopean tiedon jakelun prosessien läpi ja toisaalta myös levittämisen verkostoissa. Erityisen huomionarvoista on myös se, että ajallinen ja geospatiaalinen kattavuus skaalautuvat CITINT-toimijoiden verkostojen kattavuuden mukaan. Ideaalitapauksessa tiettyä ilmiötä käsittelevää aineistoa ja havaintoja voidaan saada laajalta alueelta tiheästi ja nopeassa tahdissa. CITINTin huomioiminen organisaatioiden toimintatavoissa voi mahdollistaa myös vuorovaikutteisuuden ja jopa räätälöityjen täsmällisten tietopyyntöjen hyödyntämisen. CITINTiä älykkäästi fasilitoimalla voidaan saavuttaa myös kansallista etua esimerkiksi koheesion lisääntymisen sekä mahdollisen subjektiivisesti koetun resilienssin vahvistavan vaikutuksen myötä. CITINTin fasilitointi voi tukea sen suorituskykyä.

Ukrainan Deltan kaltaiset nopean päivityssyklin ja laajan käyttäjäkunnan työkalut voivat mahdollistaa edun strategisella, operatiivisella ja taktisella tasolla. Delta tukee horisontaalista informaation levittämistä sekä ehjän ja strukturoidun tilannekuvan muodostamista päätöksenteon tueksi.

Todennäköisesti sekä valtiosta erilliset CITINT-toimijat että valtion tekemä CITINT-fasilitointi lisääntyvät sen mukaan, mitä epävarmemmaksi käy maailmanpoliittinen tilanne. Kuvaan tulee vielä molemmin puolin lisääntyvä vastapuolen disinformaatio ja muut tiedon luotettavuuteen, eheyteen ja saatavuuteen vaikuttavat tekijät.

Tulemme myös näkemään CITINTiä yhä enemmän ei-valtiollisessa ammatillisessa toiminnassa kuten rekrytoinnissa, konsultoinnissa, journalismissa, tieteessä ja yksityissektorin turva-alalla. Miten varmistamme, että tiedustelua tehdään eri aloilla vastuullisesti ja Suomen lakeja kunnioittaen? Entä miten tämä kehitys huomioidaan tulevaisuuden lainsäädännössä?

Lähteet

2NS. (n.d.). Open source intelligence. Haettu 1.3.2024 osoitteesta https://www.2ns.fi/palvelut/open-source-intelligence/

Althoff, M. (2026). Human intelligence. Teoksessa M. Lowenthal & R. Clark (toim.), *The 5 Disciplines of Intelligence Collection* (s. 45–79).

Arthur, P. & Cowell-Meyers, K. (2023). Irish Republican Army. Encyclopaedia Britannica. Haettu 1.10.2023 osoitteesta https://www.britannica.com/topic/Irish-Republican-Army

Borger, J. (18.12.2022). 'Our weapons are computers': Ukrainian coders aim to gain battlefield edge. The Guardian. https://www.theguardian.com/world/2022/dec/18/our-weapons-are-computers-ukrainian-coders-aim-to-gain-battlefield-edge

Burke, P. (2022). The issues in the collection, verification and actionability of citizen-derived and crowdsourced intelligence during the Russian invasion of Ukraine, 2022. *Strategic Panorama*, erikoisnumero, 94–103. https://doi.org/10.53679/2616-9460.specialissue.2022.09

Clock & Cloud. (n.d.). About us. Haettu 15.4.2024 osoitteesta https://www.ccintel.fi/en/about

Collin, P. (2020). Turun 17 vuoden takaisesta arvokuljetusryöstön yrityksestä vaaditaan yli seitsemän vuotta vankeutta – vahvin todiste hanskoista löytynyt DNA. https://yle.fi/a/3-11200771

Court, E. (20.9.2023). Military intelligence: Crowdfunded satellite had 'very important role' in Sevastopol attack. The Kyiv Independent. https://kyivindependent.com/military-intelligence-crowdfunded-satellite-had-very-important-role-in-attack-on-sevastopol/

Cyberwatch Finland. (n.d.). Yritys. haettu 15.4.2024 osoitteesta https://www.cyberwatchfinland.fi/yritys

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human factors*, 37 (1), 32–64.

EU. (2021). European Convention on Human Rights. European Court of Human Rights. Haettu 4.11.2023 osoitteesta https://www.echr.coe.int/documents/d/echr/Convention_ENG

Finder. (n.d.). Iceye Oy. Yrityshakemisto. Haettu 1.10.2023 osoitteesta https://www.finder.fi/Kaavoitus+ja+maankäytönsuunnittelu/Iceye+Oy/Espoo/yhteystiedot/2927748

Finlex (1999). Perustuslaki 731/1999. https://www.finlex.fi/fi/laki/ajantasa/1999/19990731

Finlex (2003). Järjestyslaki 612/2003. https://www.finlex.fi/fi/laki/ajantasa/2003/20030612

Finlex (2011). Esitutkintalaki 805/2011. https://www.finlex.fi/fi/laki/ajantasa/2011/20110805

Finlex (2018). Tietosuojalaki 1050/2018. https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

Fornusek, M. (11.7.2023). Minister: Ukrainian Delta system ready to integrate Western equipment, including F-16 jets. The Kyiv Independent. https://kyivindependent.com/minister-ukrainian-delta-system-ready-to-integrate-western-equipment-including-f-16/

Ghioni, R., Taddeo, M., & Floridi, L. (2023). Open source intelligence and AI: a systematic review of the GELSI literature. *AI & SOCIETY*. https://doi.org/10.1007/s00146-023-01628-x

Global Investigative Journalism Network. (n.d.) Global Conferences. Haettu 15.11.2023 osoitteesta https://gijn.org/global-conferences/

Gupta, A. (2024). Market Research Future. (n.d.). Open Source Intelligence Market Size. https://www.marketresearchfuture.com/reports/open-source-intelligence-market/market-size

Hakonen, K. (2020). Tiedustelun oikeuslähteet ja tiedustelua koskevan sääntelyn johdonmukaisuus. Kolumni. *Tiedusteluvalvontavaltuutettu*. https://tiedusteluvalvonta.fi/-/tiedustelun-oikeuslahteet-ja-tiedustelua-koskevan-saantelyn-johdonmukaisuus

Higgins, E. (2021). *Me olemme Bellingcat — Tiedustelupalvelu verkossa*. Docendo.

Iceye. (n.d.). Iceye story. Haettu 7.11.2023 osoitteesta https://www.iceye.com/company.

Inhunt. (n.d.). Suorahaku – headhunting. Haettu 7.11.2023 osoitteesta https://inhunt.fi/suorahaku-headhunting/

Isokangas, J. (2023a). Tiedustelun perusteet. Johdanto. Luentomateriaali. Haettu 25.10.2023 osoitteesta https://moodle.jyu.fi/pluginfile.php/1380866/mod_resource/content/2/01_TSAS7031s23_johdanto.pdf

Isokangas, J. (2023b). Informaatio ja tiedusteluprosessi. Luentomateriaali. Haettu 15.11.2023 osoitteesta https://moodle.jyu.fi/pluginfile.php/1386718/mod_resource/content/1/02_TSAS7031s23_informaatio_ja_prosessi.pdf

Isokangas, J. (2023c). Henkilötiedustelu ja vastatiedustelu. Luentomateriaali. Haettu 25.10.2023 osoitteesta https://moodle.jyu.fi/pluginfile.php/1394939/mod_resource/content/3/05_TSAS7031s23_HUMINT.pdf

Isokangas, J. (2023d). Tiedustelun kansainvälinen yhteistoiminta. Luentomateriaali. Haettu 25.10.2023 osoitteesta https://moodle.jyu.fi/pluginfile.php/1401286/mod_resource/content/1/TSAS7031s23_KVYT.pdf

Isokangas, J. (2024). Sähköposti työryhmälle.

Journalisti (anonyymi) (2023). Haastattelu 15.11.2023.

Kajanmaa, P. (2022). [MPKK:n sotataidon laitoksen johtajan Twitter-viesti, jossa kerrotaan tiedusteluyhteistyöstä Black Bird Groupin kanssa.] Haettu 25.10.2023 osoitteesta https://twitter.com/PutteKaj/status/1502754325994647555?s=20.

Kastehelmi, E (2023). Haastattelu 17.10.2023.

Kerttunen, M. (2007). *Strategia*. Julkaisusarja 3, Strategian asiatietoa, no 4, 2007. Maanpuolustuskorkeakoulu, Strategian laitos. http://www.urn.fi/URN:NBN:fi-fe201201241125

Lapinkangas, E. & Julkunen, P. (2022). Dronehavaintoja tulee nyt ennätystahtia – toimi näin, jos näet jotain epäilyttävää. Ilta-Sanomat. https://www.is.fi/kotimaa/art-2000009152128.html

Laulajainen, A., Taivalmaa, A., Vilén, T. & Virtanen M. (2023). Valtiollisen tiedustelumonopolin murtuminen. Teoksessa J. Isokangas (toim.), *Tiedustelun maailma: Muuttuva tiedustelu*. Tiedusteluanalyysi I -kurssin raportteja (s. 9–24). Informaatioteknologian tiedekunnan julkaisuja, 98. Jyväskylän yliopisto. https://jyx.jyu.fi/bitstream/handle/123456789/86797/1/Tiedustelun%20maailma%20-%20Muuttuva%20tiedustelu.pdf#page=9

Leponen, M. (2023). Haastattelu 15.11.2023.

Lowenthal, M & Clark, R (2016). *The Five Disciplines of Intelligence Collection*. SAGE.

Lozovenko, T. (11.7.2023). Ukraine's Delta system passes NATO tests and can integrate F-16s. *Ukrainska Prav*da. https://www.pravda.com.ua/eng/news/2023/07/11/7410815/

Lyytikkä, J. & Hallamaa, T. (2018). Kiina rakentaa verkkoa maailmalle – Googlen ex-toimitusjohtaja ennustaa, että Kiinan vaikutusvallan kasvu jakaa internetin kahtia. *Yle*. https://yle.fi/a/3-10442069

Maanpuolustuskorkeakoulu. (2019). Kadettikoulutuksen mahdollistajat. Kolumni. https://maanpuolustuskorkeakoulu.fi/-/kadettikoulutuksen-mahdollistajat

McDowell, D. (2008). *Strategic intelligence: a handbook for practitioners, managers, and users* (Vol. 5). Scarecrow Press.

Malkki, L. (2014). Toisen terroristi, toisen vapaustaistelija – Terrorismin määrittelyn ongelmat. Teoksessa A. Paronen & O. Teirilä (toim.), *Vihatkoot kunhan pelkäävät. Näkökulmia terrorismiin ilmiönä* (s. 15–42). MPKK:n strategian laitos. https://www.doria.fi/bitstream/handle/10024/100080/Vihatkoot%20kunhan%20pelkäävät%20verkko-1.pdf?sequence=2&isAllowed=y

Militarnyi. (27.10.2022). *Ukraine unveiled its own Delta situational awareness system*. https://mil.in.ua/en/news/ukraine-unveiled-its-own-delta-situational-awareness-system/

Militarnyi. (4.2.2023). *The Defense Forces of Ukraine to introduce the Delta system*. https://mil.in.ua/en/news/the-defense-forces-of-ukraine-to-introduce-the-delta-system/

Militarnyi. (9.3.2023). *Ukrainian Intelligence showcases images from ICEYE satellite, funded by local donations*. https://mil.in.ua/en/news/ukrainian-intelligence-showcases-images-from-iceye-satellite-funded-by-local-donations/

Mint Security. (n.d.). OSINT lyhyesti. Haettu 1.3.2024 osoitteesta https://www.mintsecurity.fi/osint/

Mitrovich, G. (2016) *Theorizing Citizen Learning of Open Source Intelligence as Tradecraft Training*. https://www.proquest.com/openview/bcb13358b8e1775f077d51abab09395b

Mäki-Kuhna, J. (2023). *Tiedustelun perusteet. Avointen lähteiden tiedustelu*. Luentomateriaali 9.10.2023. https://moodle.jyu.fi/pluginfile.php/1402796/mod_resource/content/3/TSAS7031-23%20OSINT%20datan%20kera%CC%88ys.pdf

Mäntysalo, J. – Pietarinen, E. (2023). KRP ja Tulli: Järjestäytynyt rikollisuus on soluttautunut Suomen satamiin – grafiikka näyttää, miten se toimii. *Yle*. https://yle.fi/a/74-20015814

Nasu, H. (2022). Targeting a Satellite: Contrasting Considerations between the Jus ad Bellum and the Jus in Bello. *International Law Studies Vol, 99*, 2022, s. 143–177.

Nasu, H. (6.9.2022). *"The eye in space": Iceye's SAR satellites and the law of war*. Lieber Institute, West Point: Articles of War. Haettu 10.10.2023 osoitteesta https://lieber.westpoint.edu/eye-space-iceyes-sar-satellites-law-of-war/

Nelliyullathil, M. (2020). Teaching Open Source Intelligence (OSINT) Journalism: Strategies and Priorities. *Communication & Journalism Research*, 9 (1), 61–73. https://cjrjournal.in/Uploads/Files/CJR%202020%20JUNE.pdf#page=74

p1ngul1n0. (2023). *Blackbird*. An OSINT tool to search fast for accounts by across 581 sites. Haettu 12.11.2023 osoitteesta https://github.com/p1ngul1n0/blackbird/blob/main/README.md

Paasonen, J. (2023). Yksityisetsivätoiminnan huomioiminen lainsäädännön kehittämisessä. Blogipostaus. https://jyripaasonen.fi/yksityisetsivatoiminnan-huomioiminen-lainsaadannon-kehittamisessa/

Pešek, K. (2023). *Komparativní případové studie: využití občanského zpravodajství (CITINT) během probíhajícího konfliktu na Ukrajině v porovnání s vybranými soudobými konflikty*. Master's thesis. Masaryk University, Faculty of Social Studies. https://is.muni.cz/th/qjy3x/

Pietilä, I. (2022). *Studies of Digital Solutions Supporting Societal Participation of Youths. Tampere University*. Doctoral dissertation. https://trepo.tuni.fi/handle/10024/143469.

Poliisi. (2023). KRP tutkii epäiltyä turvallisuussalaisuuden paljastamista - kolmea vaaditaan vangittavaksi. https://poliisi.fi/-/krp-tutkii-epailtya-turvallisuussalaisuuden-paljastamista-kolmea-vaaditaan-vangittavaksi

Puolustusvoimat. (n.d.). Puolustusvoimien tiedustelulaitos. Haettu 17.11.2023 osoitteesta https://puolustusvoimat.fi/tietoa-meista/tiedustelulaitos

Rikoslaki 39/1889. https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Saini Fasanotti, F. (2022). Russia's Wagner Group in Africa: Influence, commercial concessions, rights violations, and counterinsurgency failure. https://www.brookings.edu/articles/russias-wagner-group-in-africa-influence-commercial-concessions-rights-violations-and-counterinsurgency-failure/

Scott, B. (2024). "Everyone freaks out when the leaks are made": data leaks, investigative journalism and intelligence practice. *Journal of Financial Crime*. Emerald Publishing Limited. https://www.emerald.com/insight/content/doi/10.1108/JFC-05-2023-0123/full/pdf?title=everyone-freaks-out-when-the-leaks-are-made-data-leaks-investigative-journalism-and-intelligence-practice

Sisäministeriö. (2017). Siviilitiedustelun ja Suojelupoliisin ohjauksen kehittäminen sisäministeriön hallinnonalalla - työryhmän raportti. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80032/Siviilitiedustelun%20ja%20Suojelupoliisin%20ohjaus_NETTI.pdf?sequence=1&isAllowed=y

Soeiro, L. (13.12.2022). BlackBird — Osint Tool. Medium.com. https://lucassoeiro.medium.com/blackbird-osint-tool-c1ed8a88c7aa.

Steele, R. D. (2002). *The new craft of intelligence: achieving asymmetric advantage in the face of nontraditional threats*. Strategic Studies Institute, US Army War College.

Suojelupoliisi. (n.d.). Supon tehtävät selkosuomeksi. Haettu 8.11.2023 osoitteesta https://supo.fi/supon-tehtavat-selkokielella

Suomen Yksityisetsivä- ja Lakitoimistoliitto. (n.d.-b). Eettiset säännöt. Haettu 7.11.2023 osoitteesta https://www.yksityisetsiva.fi/?page_id=207

Teti, A. (2012). Intelligence of the third millennium – The 'Citizen Intelligence'. *Gnosis* 4/2012. Agenzia Informazioni e Sicurezza Interna. https://gnosis.aisi.gov.it/

Tilastokeskus. (2008). Toimialaluokitus 2008. https://www2.tilastokeskus.fi/fi/luokitukset/toimiala/

Tutkivan journalismin yhdistys (2023). Tutki!2023 puhujat. https://tutkikonferenssi.fi/puhujat/

Tutkivan journalismin yhdistys. (2011). Yhdistyksen säännöt. Haettu 25.10.2023 osoitteesta https://www.tutkiva.fi/wp-content/uploads/2023/05/YhdistyksenSaannot.pdf

Ulkoasiainministeriö. (2015). Sodan oikeussäännöt. Ulkoasiainministeriön julkaisuja 5/2015. https://um.fi/documents/35732/48132/julkaisu__sodan_oikeussäännöt

Vainio, K. (27.5.2021). Tiedustelun renessanssi – järjestöt ja yritykset haastavat tiedustelupalveluiden monopolin. *Ulkopolitiikka*. https://ulkopolitiikka.fi/lehti/2-2021/tiedustelun-renessanssi/

Vapa, M. (2023). [Marko Vapa -kanavan sittemmin poistettu Youtube-video.] Haettu 11.4.2023 osoitteesta https://www.youtube.com/watch?v=JiVfAFcuP9w

Vähätalo, E. (2019). Jyväskylän kybermaistereilla riittää kysyntää. Ruotuväki-lehti. https://ruotuvaki.fi/-/jyvaskylan-kybermaistereilla-riittaa-kysyntaa

Walton, A. (2013). Financial Intelligence: Uses and Teaching Methods (Innovative Approaches from Subject Matter Experts). *Journal of Strategic Security, 6 (3)*, 393–400. https://www.jstor.org/stable/10.2307/26485084

Wikén, E. & Salihu, D. (2023). Uppgifter: Anställd på domstol varnade kriminella om avlyssning. Sveriges Television. https://www.svt.se/nyheter/inrikes/sa-infiltrerar-kriminella-den-offentliga-sektorn

Yksityisetsivä (n.d, -a). Suomen Yksityisetsivä- ja Lakitoimistoliitto. Etusivu. Haettu 7.11.2023 osoitteesta https://www.yksityisetsiva.fi/