Sami Siljoranta

# AVOINTEN LÄHTEIDEN TIEDUSTELUN TARKASTELU TIEDUSTELULAKIEN NÄKÖKULMASTA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

# TIIVISTELMÄ

Siljoranta, Sami
Avointen lähteiden tiedustelun tarkastelu tiedustelulakien näkökulmasta
Jyväskylä: Jyväskylän yliopisto, 2020, 91 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Kari, Martti

Tutkimuksen tavoitteena on selvittää mitä tiedustelulaeissa ja niiden esitöissä sanotaan avointen lähteiden tiedustelusta. Tutkimuksen tarkoituksena on myös kuvata lainsäädännön nykytila tässä kontekstissa. Tutkimuksen tutkimusmenetelmänä käytetään aineistolähtöistä sisällönanalyysiä. Tutkimuksen tuloksena muodostuu käsitejärjestelmä, joka kuvaa tiedustelulakien ja niiden esitöiden sisältöä informatiivisessa muodossa suhteessa sääntelemättömiin tiedonhankintakeinoihin. Lainsäädäntö ottaa hyvin neutraalisti kantaa avointen lähteiden tiedusteluun ja tietoverkkoja koskevaan toimintaan ylipäätään. Lainsäädäntöön tulisi jatkuvasti kohdistaa yksityiskohtaista tarkastelua, jotta se kykenee vastaamaan maailmassa vallitseviin ilmiöihin, kuten voimistuneeseen digitalisaatioon. Tutkimuksen tuloksista selviää myös se, kuinka avointen lähteiden tiedustelua käytetään tiedustelutoiminnan tukena, ohjaajana ja tehostajana.

Asiasanat: OSINT, avointen lähteiden tiedustelu, lainsäädäntö, sisällönanalyysi

# ABSTRACT

Siljoranta, Sami
Examining open-source intelligence from the perspective of intelligence regulation
Jyväskylä: University of Jyväskylä, 2020, 91 pp.
Cyber Security, Master's Thesis
Supervisor(s): Kari, Martti

The goal of the study is to find out what the intelligence laws and their preliminary work say about open-source intelligence. The purpose of the study is also to describe the current state of the legislation in this context. Data-driven content analysis is used as the research method in this study. As a result, a conceptual system is formed that describes the content of intelligence laws and their preliminary work in an informative form in relation to unregulated methods of obtaining intelligence. The legislation takes a very neutral stance on open source intelligence and network operations in general. Legislation should be a subject to constant examination to be able to respond to global phenomena such as increased digitalization. The results of this study also show how open source intelligence is used to support, guide, and enhance intelligence operations.

Keywords: OSINT, open source intelligence, legislation, content analysis

# KUVIOT

# SISÄLLYS

# 1 JOHDANTO

Tässä luvussa käsitellään tutkimuksen taustaa ja tutkimuksen tavoitteita. Tässä luvussa myös esitellään tutkimuksen tärkeimmät käsitteet, joita käsitellään tarkemmin luvussa 2. Lisäksi tässä luvussa esitellään tutkimusongelma ja -kysymykset, aiheen rajaus, tutkimuksen rakenne sekä aiempia tutkimuksia.

## 1.1 Tutkimuksen tausta ja tavoitteet

Tiedusteluviranomaisilta vaaditaan nykyään huomattavan paljon kykyä sopeutua uusin uhkiin ja vaikuttamisen malleihin, sillä nykyään käytetään laajasti erilaisia hybridivaikuttamisen keinoja ja informaatio-operaatioita (Lohse & Viitanen, 2019, s. 239). Näitä erilaisia perinteisistä vaikuttamisen keinoista poikkeava keinoja on kohdistettu laajasti Euroopan maihin, ja turvallisuustilanne on laajasti muuttunut sekä siirtynyt entistä pohjoisemmaksi (Lohse & Viitanen, 2019, s. 240). Suomessa tiedustelulait astuivat voimaan vuonna 2019, mutta tätä ennen varsinaista tiedustelulainsäädäntöä ei ole ollut (Lohse & Viitanen, 2019, s. 17). Tällä lainsäädännön muutoksella pyritään vastaamaan tiedusteluviranomaisten mahdollisuuteen toteuttaa lakisääteisiä tehtäviään.

Informaatioavaruus on laajempi, kuin mitä yleisesti voidaan koskettaa, tuntea tai nähdä ja täten on mahdotonta käsittää sen todellista laajuutta (Olcott, 2012, s. 104). Kylmän sodan aikaan kaikesta tiedustelutiedosta vain 10 % oli kerätty avoimista lähteistä, mutta nykyään tilanne on päinvastainen, sillä arvioiden mukaan jopa 90 % tiedustelutiedosta kerätään avoimista lähteistä (Akhgar, ym., 2016, s. 54). Avointen lähteiden tiedustelua (engl. OSINT, Open Source Intelligence) suoritetaan joko yksinään tai jonkin toisen tiedustelulajin tukena. Tiedustelulajeja käsitellään tarkemmin luvussa 2, käsitteiden määrittelyn yhteydessä.

Hallituksen esityksen HE 203/2017 mukaan avointen lähteiden tiedusteluksi katsotaan yleisesti sellainen toiminta, joka ei loukkaa kohteen yksityisyyden suojaa tai luottamuksellisen viestin salaisuutta ja avointen lähteiden tiedustelua ei voida myöskään määritellä sellaiseksi toiminnaksi, josta perustuslain

mukaan olisi säädettävä lailla (HE 203/2017). Avointen lähteiden tiedustelusta voidaan käyttää nimitystä kodifioimaton tiedustelumenetelmä, jolla viitataan tavanomaisoikeuden piiriin kuuluviin menetelmiin (Lohse & Viitanen, 2019, s. 243). Käytännössä tämä voidaan tulkita siten, että mikään keskeisnormisto ei avointen lähteiden tiedustelua säätele. Työ tiedustelun oikeus- ja tarkoituksenmukaisuuskysymysten parissa on päättymätön ja näitä kysymyksiä tulisi jatkuvasti arvioida sekä valtaa pitävien instituutioiden sisällä, että tiedeyhteisöissä ja mediassa (Lohse & Viitanen, 2019, s. 5).

Tässä tutkimuksessa tutkitaan, mitä avointen lähteiden tiedustelusta sanotaan Suomen tiedustelulaeissa. Tutkimuksen kohteena ovat varsinaisten lakien lisäksi myös lakien taustalla olevat esityöt. Suomessa laki sotilastiedustelusta määrittelee tiedustelua Puolustusvoimien osalta ja poliisilain luku 5 a määrittelee siviilitiedustelua. Avointen lähteiden tiedustelu on tiedustelutoiminnan erityistapaus ja se lasketaan tavanomaisoikeuden piiriin. OSINT:ia ei suoraan lainsäädännössä määritellä, joten mielenkiinto kohdistuu erityisesti lakien esitöihin, joista tässä tutkimuksessa etsitään vastauksia tutkimusongelmaan. Aihetta ei ole laajasti tutkittu, joka tekee myös tutkimusaiheesta mielenkiintoisen. Aiempien tutkimusten ja julkaisujen esittelyn yhteydessä käy myös ilmi se, että OSINT:n osalta kaivataan lisää tutkimusta lainsäädännön näkökulmasta. Taustan ja tutkimuksen määrittelyn perusteella tärkeimmät perustelut tutkimuksen tarpeellisuudesta ovat tiivistettynä lainsäädännön neutraalius ja vähäiset tutkimukset aiheesta. Tutkimuksen tavoitteena on selvittää, mitä tiedustelulaeissa esitöineen sanotaan avointen lähteiden tiedustelusta.

Tässä tutkimuksessa tutkitaan ajankohtaan ja tarpeeseen nähden tärkeitä aihealueita, jotka ovat myös aiemmassa kirjallisuudessa tunnistettuja aihealueita. Lisäksi akateemisessa mielessä myös 9/11-tapahtumat antoivat huomattavasti lisäpotkua tiedustelun tutkimukselle ja tämän seurauksena on ilmestynyt paljon arvokkaita tutkimuksia teoreettisiin, metodologisiin ja koulutuksellisiin ongelmiin liittyen (Gruszczak, 2016, s. 50).

## 1.2 Keskeiset käsitteet

Tutkimuksen keskeisimmät käsitteet ovat tiedustelu, tiedustelulaji, avointen lähteiden tiedustelu (OSINT) ja avoimet lähteet. Tiedustelu on tämän tutkimuksen yläkäsite, joka kuvaa laajemmin tutkittavaa aihepiiriä. Tiedustelulajeja, joita tiedustelu pitää sisällään, on useita, joista yksi on avointen lähteiden tiedustelu. Olennainen käsite tutkimuksen kannalta on myös ”avoimet lähteet”, joka kuvaa mitä avoimilla lähteillä tarkoitetaan. Keskeisien käsitteiden ja tutkimusaiheen määrittelyä on tehty syvällisemmin luvussa 2.

## 1.3 Tutkimusongelma ja aiheen rajaus

Tutkimuksen päämääränä on selvittää, mitä avointen lähteiden tiedustelusta sanotaan tiedustelulaeissa. Lisäksi tavoitteena on selvittää, mitä laeista käy ilmi liittyen avointen lähteiden tiedustelun tukevaan rooliin tiedustelutoiminnassa. Tutkimuksessa tarkasteltavat lait rajataan selkeästi tiedustelulainsäädäntöön ja kaikki muut lait jätetään tässä tutkimuksessa tarkastelun ulkopuolelle. Tutkimuksessa tarkastellaan myös tarkastelun kohteena olevien lakien esitöitä. Näiden määrittelyjen perusteella muodostetaan tutkimuskysymys (1) ja sitä tukeva apukysymys (2):

1. Mitä sotilas- ja siviilitiedustelulaissa sanotaan avointen lähteiden tiedustelusta?

2. Mitä laeista käy ilmi liittyen avointen lähteiden tiedustelun tukevaan rooliin tiedustelutoiminnassa?

## 1.4 Tutkimuksen rakenne

Tutkimuksen ensimmäisessä luvussa esitellään tutkimuksen taustaa ja tavoitteita sekä keskeisiä käsitteitä ja tutkimusongelmaa. Ensimmäisessä luvussa myös käsitellään tämän tutkimuksen kannalta olennaisia aiempia tutkimuksia ja julkaisuja. Tutkimuksen luvussa 2 käsitellään tutkimuksen kannalta tärkeimpiä käsitteitä ja aihepiirejä. Luvussa 3 käsitellään tutkimuksen aineistoa, tutkimusmenetelmää ja tutkimusprosessia. Neljännessä luvussa esitellään tutkimuksen tuloksia ja tutkimuksen käytännön toteutusta. Tutkimuksen luvussa 5 esitellään johtopäätökset, jotka tuloksista nousevat. Viimeisessä luvussa käsitellään tutkimuksen toteuttamista, luotettavuutta ja jatkotutkimustarpeita.

## 1.5 Aiempi tutkimus

Avointen lähteiden tiedustelu on tiedustelun erityistapaus, eikä sitä laissa säädellä. Avointen lähteiden tiedustelua on myös tutkittu hyvin vähän lainsäädännön näkökulmasta. Joitain tutkimuksia ja julkaisuja on kuitenkin tarjolla, joissa mainitaan lainsäädännön roolista tässä kontekstissa. Esimerkiksi Vaskin (2018) on tutkinut yksityisyyden suojaa OSINT:ssa.

Useissa kirjoissa ja tutkimuksissa (ks. esimerkiksi Bazzell, 2019 tai Akhgar, Bayerl ja Sampson, 2016) OSINT :ia käsitellään pääasiassa sen teknisen toteuttamisen näkökulmasta (ks. myös esimerkiksi Tuominen, 2019 tai Tolppanen, 2020). Akhgar ja muut (2016) ovat kuitenkin pohtineet myös OSINT:n ja yksityisyyden suojan välistä yhteyttä. Akhgarin ja muiden (2016) mukaan Hill ja Davis ovat jo

vuonna 2013 pohtineet, että lainsäädännölliset epävarmuudet ympäröivät avointen lähteiden tiedustelua, sillä tätä toimintaa käsittelevissä oikeuskäytännöissä on puutteita (Akhgar, ym., 2016, s. 281). Bazzell on käsitellyt kirjassaan (2019) peitetaktiikoita osana OSINT:ia. Hänen mukaansa Yhdysvaltojen tuomioistuimet ovat johdonmukaisesti hyväksyneet peitetaktiikoiden käyttöä Internetissä. Tämä perustuu siihen olettamukseen, että jokainen järjissään oleva Internetin käyttäjä ymmärtää sen tosiasian, että muut Internetin käyttäjät eivät välttämättä esiinny siellä omana itsenään. Peitetaktiikat ovat mielenkiintoinen osa OSINT:ia, mutta Bazzell ei ole kirjassaan tätä aihetta tutkinut sen tarkemmin lainsäädännön näkökulmasta, vaikka aiheeseen liittyvää yksityisyysnäkökulmaa kirjassa sivutaankin.

Johnson (2013) on käsitellyt lainsäädännön osuutta OSINT:ssa. Lainsäädännölliset ja eettiset näkökulmat liittyen avointen lähteiden tiedusteluun käyvät kilpajuoksua ripeästi kehittyvän sosiaalisen median palvelutarjonnan kanssa, erityisesti siksi, että sosiaalisen median palvelut ja niiden käyttöehdot eroavat laajalti toisistaan (Johnson, 2013, s. 223).

Myös esimerkiksi Lohse ja Viitanen (2019) ovat käsitelleet yleisesti tiedustelua eettisestä ja lainsäädännöllisestä näkökulmasta, mutta lainsäädännön käsittely on pidetty lähinnä yleisellä tasolla. Heidän mukaansa kansallisen lainsäädännön lisäksi tulee ottaa huomioon myös Euroopan yleiset sopimukset, kuten EU:n tietosuoja-asetus (engl. *GDPR – General Data Protection Regulation*) ja Euroopan ihmisoikeussopimus, jonka toteutumista valvoo Euroopan ihmisoikeustuomioistuin (EIT) (Lohse & Viitanen, 2019, s. 127). Perusoikeudet Euroopan Unionin laajuisesti taas on määritelty EU:n perusoikeuskirjassa (Lohse & Viitanen, 2019, s. 133).

Gibson (2011) on pohtinut OSINT:ia myös datan analysoinnin näkökulmasta siten, että tiedon rikastus voi tuottaa arkaluontoista tietoa. Avoimista lähteistä saadun datan analysointi saattaa tuottaa tietoa, joka voidaan luokitella arkaluontoiseksi ja lisäksi tiedon keräyksen keinot voivat olla anonymisoituja (Gibson, 2011, s. 77). Gibson on myös pohtinut yksityisyysnäkökulmaa OSINT:ssa.

Lainsäädännöllisestä näkökulmasta kaivataan linjauksia, ja Yhdysvaltain tiedusteluyhteisö IC *(Intelligence Community)* onkin vakiinnuttanut position avointen lähteiden osalta (engl. *Assistant Director of National Intelligence for Open Source*) ja perustanut kansallisen avointen lähteiden keskuksen (engl. *National Open Source Center*) (Akhgar, ym., 2016, s. 54). Tammikuussa 2014 on perustettu *The Global Commission on Internet Governance*, jonka tavoitteena on selkeyttää ja edistää strategisella tasolla Internetin hallinnollisia näkökulmia (Omand, 2015, s. 6). Kyseinen taho on myös määritellyt tietyt olennaiset teemat, joihin he erityisesti ovat keskittyneet. Teemoja ovat hallintotavan legitiimiyden lisääminen, ekonomisten innovaatioiden ja kasvun kannustaminen, ihmisoikeuksien varmistaminen verkossa sekä systemaattisten riskien ehkäiseminen (Omand, 2015, s. 6). Omand (2015) toteaa, että modernin tiedustelutoiminnan pohjana tulisi käyttää ihmisoikeussopimusten kunnioittamista (Omand, 2015, s. 7). Keskustelua siitä, kuinka Internetiä tulisi hallinoida lainsäädännöllisestä näkökulmasta on

kiihdyttänyt esimerkiksi ns. *Snowden* –paljastus (*The Snowden Affair*), jossa Edward Snowden paljasti asiakirjoja tarkkailumenetelmistä (Richelson, 2013).

Nykyään avointen lähteiden tiedustelulla viitataan usein suoranaisesti avointen lähteiden Internet-tiedusteluun, jossa tiedonhakukanavana käytetään vain Internetiä (ks. esimerkiksi Akhgar, ym., 2016 tai Williams & Blum, 2018). Avointen lähteiden tiedustelua myös nykyään pilkotaan osiin, tai kutsutaan eri lyhenteillä. Aiheeseen liittyvissä julkaisuissa ja tutkimuksissa esiintyy useita eri lyhenteitä, joita ovat muun ohella *WEBINT – Web Intelligence* (ks. Putting Data in Perspective With Web Intelligence, 2014), *SOCMINT – Social Media Intelligence* (ks. esimerkiksi Şuşnea & Iftene, 2018), *DIGITAL HUMINT – Digital Human Intelligence* (ks. Lombardi, Rosenblum & Burato, 2015), *OSINT – Open Source Intelligence* ja *SI – Social Intelligence* (ks. Casanovas, 2014). Lyhenteet ovat lisääntyneet tiedusteluympäristön ja OSINT:n muutoksen myötä. Sosiaalisen median merkittävät komponentit, kuten käyttäjien luoma sisältö ja kuluttajien luoma media nähdään suurimpina määrittelijöinä Web 2.0 -käsitteelle, josta myös nykyään puhutaan tässä kontekstissa (Zeng, Chen, Lusch & Li, 2010). Myös Williams ja Blum (2018) ovat pohtineet OSINT:n muutosta tutkimuksessaan ja heidän mielestään tulisikin puhua toisen sukupolven OSINT :sta (Williams & Blum, 2018, s. ix). Williams ja Blum (2018) ovat myös pohtineet tukimusraportissaan tiedustelulajien leikkaavuutta, joka on merkittävä mielenkiinnon kohde OSINT :n lainsäädännössä.

Valitettavasti OSINT:ia käytetään paljon myös rikolliseen tarkoitukseen ja pahantekoon, kuten häirintään ja kiusaamiseen. Tähän liittyen ainakin Yhdysvalloissa on otettu kantaa lainsäädännöllisellä tasolla termein ”*Cyber-stalking*” ja ”*Cyber-bullying*”.

Suomessa tiedustelulakeja on tutkittu jonkin verran, eri näkökulmista. Esimerkiksi Kurttila (2015) on tutkinut Pro gradu -tutkielmassaan tiedusteluun liittyvää ymmärrystä julkisessa keskustelussa. Myös Koskela (2018) on tutkinut Pro gradu -tutkielmassaan tiedustelulakihankkeen käsittelyä Suomen medioissa. Helenius (2020) taas on keskittynyt Pro gradu -tutkielmassaan tiedustelulakiprosessin viimeiseen työvaiheeseen eduskuntatyöskentelyssä ja sen aikana tiedustelulaeista esitettyihin näkemyksiin. Tiedustelusääntelyä on tutkinut myös esimerkiksi Havulinna (2018) Pro gradu -tutkielmassaan. Forss (2019) taas on tutkinut salaisia tiedonhankinta- ja pakkokeinoja poliisi- ja peiteprofiileilla. Juutilainen (2008) taas on tutkinut OSINT:ia sotilastiedustelussa, mutta tutkimuksen tavoitteena oli selvittää, mikä OSINT:n rooli on tiedusteluprosessissa. Myös Lammi (2017) on tutkinut OSINT:n roolia strategisessa sotilastiedustelussa. Doria -julkaisuarkistosta löytyy myös muutamia muita tutkimuksia OSINT:sta, mutta merkittävää lainsäädännöllistä tarkastelua ei ole tehty.

Suomessa toteutetut tutkimukset tiedustelulakien osalta keskittyvät lähinnä aiheen tiimoilta käytyihin keskusteluihin medioissa ja avointen lähteiden tiedustelua on tutkittu hyvin niukasti. Viime vuosien aikana kuitenkin kiinnostus tiedustelua ja tiedustelulakeja kohtaan on kasvanut ja joitain tutkimuksia on ilmestynyt. Avointen lähteiden tiedustelua lainsäädännöllisistä näkökulmista on

tutkittu kattavammin Suomen ulkopuolella ja useissa julkaisuissa todetaan lainsäädännöllisten epävarmuuksien ympäröivän avointen lähteiden tiedustelua.

# 2 TIEDUSTELUTOIMINTA

Tässä luvussa määritellään tutkimuksen kannalta olennaisia käsitteitä, jotka esiteltiin aiemmin ensimmäisessä luvussa. Tutkimuksen aihepiirin määrittely aloitetaan tiedustelun käsitteestä ja luvun lopussa määrittely kohdistetaan tarkemmin avointen lähteiden tiedustelun käsitteeseen.

## 2.1 Tiedustelu

Tiedustelulle ei ole olemassa yhtä yleisesti hyväksyttyä määritelmää, vaan jokainen tiedustelua harjoittava, tutkiva tai opettava taho määrittelee sen omista lähtökohdistaan. Tässä tutkimuksessa tiedustelu tarkoittaa prosessia, joka tuottaa informaatiota kohteesta ja olosuhteista strategisen suunnittelun, rikostutkinnan ja hallitusten, yleisen järjestyksen ylläpitämiseen tarkoitettujen organisaatioiden ja liike-elämän käyttöön tilannekuvan muodostamiseksi ja päätöksenteon tueksi. Prosessiin kuuluu datan keräys, analyysi, raportointi ja valmiin tiedustelutuotteen jakelu asiakkaalle tämän tietopyynnön mukaisesti sekä tämän prosessin johtaminen, kehittäminen ja laadunvalvonta. (Kari, 2019.)

Vakiintunut valtiollinen tiedustelutoiminta on koko historian mittakaavassa tuore käsite, mutta tiedon tarpeeseen on pyritty vastaamaan jo tuhansien vuosien ajan (Porvali, 2018, s. 10). Tiedusteluviranomaiset jaetaan sotilas- ja siviilitiedustelupalveluihin ja valtiollisella tiedustelutoiminnalla tarkoitetaan tiedon tuottamista kansalaisten- ja demokraattisten rakenteiden suojelemiseksi (Porvali, 2018, s. 11).

Tiedustelua voidaan yleisesti myös määritellä siten, että yksittäinen tiedonhaku ei vielä tee toiminnasta tiedustelua, mutta tiedonhankinnan järjestelmällisyys ja sidonnaisuus päätöksentekoon täyttävät tiedustelutoiminnan tunnusmerkit (Porvali, 2018, s. 13). Tiedustelutoiminnassa puhutaan myös strategisesta tiedustelusta. Strategisella tiedustelulla tarkoitetaan tavoitteellista informaation ja datan käsittelyä sekä rikastamista siten, että meneillään olevia tapahtumia kyetään ennustamaan luotettavasti ja tehokkaasti (Gruszczak 2016, s. 37). Tiedustelun tehtävänä on myös tuottaa sellaista tietoa, joka perustuu faktoihin, tarkistettuihin havaintoihin ja pohdintoihin niistä sekä kumota vääriä mielikuvia (Porvali, 2018, s. 14).

Lain näkökulmasta Suomen viralliset tiedustelun määritelmät vastaavat esimerkiksi Yhdysvaltojen ja Ruotsin virallisia käsityksiä tiedustelun määrittelemisestä (Lohse & Viitanen, 2019, s. 37). Tiedustelussa on yleisesti kyse toiminnasta, prosessista, tuotteesta tai organisaatiosta ja tiedustelun tavoitteena on kansallisen turvallisuuden suojaaminen sekä tiedon tuottaminen päätöksenteon tueksi. Suomen kansallisessa lainsäädännössä tiedustelua määritellään joko siviilitiedusteluksi tai sotilastiedusteluksi. Lainsäädännön perusteella siis toimivaltuudet ja tehtävät kuuluvat yksiselitteisesti suojelupoliisille ja Puolustusvoimille

(Lohse & Viitanen, 2019, s. 51). Tarkemmin Suomen kansallinen tiedustelu- ja turvallisuuspalveluyhteisö voidaan määritellä siten, että siihen kuuluvat suojelupoliisi, pääesikunta ja Puolustusvoimien tiedustelulaitos, mutta sotilastiedustelua harjoitetaan lisäksi kauttaaltaan Puolustusvoimissa sotilastiedusteluviranomaisen alaisena (Lohse & Viitanen, 2019, s. 53).

### 2.1.1 Tiedustelulait

Tiedustelua säädellään laissa sekä kansallisella tasolla, että kansainvälisellä tasolla ihmisoikeusvelvoitteiden muodossa ja lisäksi tiedustelun normistoon kuuluu tavanomaisoikeutena muun ohella avointen lähteiden tiedustelu (Lohse & Viitanen, 2019, s. 23). Tavanomaisoikeudellisiin tiedustelumenetelmiin voidaan lukea tarkkailu, avointen lähteiden tiedustelu, kuvaustiedustelu ja geotiedustelu (Lohse & Viitanen, 2019, s. 109).

Lohsen ja Viitasen (2019) mukaan Suomen tiedustelulainsäädäntöä voidaan pitää reaktiona muuttuneisiin ja heikentyneisiin Suomen ulkopuolisiin olosuhteisiin. Tiedustelusääntelyllä haluttiin parantaa erityisesti näkyvyyttä vieraaseen sotilaalliseen toimintaan ja vakavasti kansallista turvallisuutta uhkaavaan toimintaan (Lohse & Viitanen, 2019, s. 240). Lainsäädännön tulkitseminen tiedustelutoiminnan yhteydessä ei aina ole yksiselitteistä ja erityisesti avointen lähteiden tiedustelun yhteydessä vaatii lainsäädännön tulkitseminen tulkitsijaltaan paljon. Uusien ilmiöiden ilmentyessä joudutaan voimassa olevaa oikeutta ja täsmentäviä ratkaisukäytänteitä pohtimaan uudelleen, sillä vallitseva oikeusjaottelu ei usein tarjoa tyydyttäviä vastauksia uusien ilmiöiden muodostamiin uusiin oikeudellisiin ongelmiin (Lohse & Viitanen, 2019, s. 241).

Yleisesti tiedustelutoiminnassa pärjätään sen omilla keskeisnormistoilla, joita ovat poliisilain 5 a luku, laki tietoliikennetiedustelusta siviilitiedustelussa, laki sotilastiedustelusta, laki tiedustelutoiminnan valvonnasta ja eduskunnan työjärjestys tiedusteluvalvontavaliokuntaa koskevin osin, eikä kyseeseen tule eri oikeudenalojen yhdisteleminen (Lohse & Viitanen, 2019, s. 243).

On tietysti olennaista tiedostaa, että tiedustelutoimintaan kokonaisuudessaan liittyy paljon erilaisia oikeuslähteitä. Tiedusteluun liittyviä oikeuslähteitä ovat myös tuomioistuimen luparatkaisut, tiedustelun ulkoisen valvonnan kannanotot, oikeustieteen tulkintasuositukset ja turvallisuusstrategiaratkaisut (Lohse & Viitanen, 2019, s. 25).

Tiedustelutoimintaa koskeva normisto koostuu kansallisesta lainsäädännöstä, kansainvälisistä ihmisoikeusvelvoitteista ja tavanomaisoikeudesta, mutta peruspilarina nähdään kansallinen lainsäädäntö, sillä EU:n sopimusten mukaan kukin jäsenvaltio on ensikädessä itse vastuussa kansallisen turvallisuuden ylläpitämisestä (Lohse & Viitanen, 2019, s. 242). On kuitenkin hyvä tiedostaa, että kansallisen lainsäädännön tulee olla linjassa kansainvälisten velvoitteiden kanssa, joita jokaisen tiedustelua suorittavan toimijan tulee toiminnassaan huomioida. Tästä syystä tiedustelutoimijoita edellytetään seuraamaan EU-tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen oikeuskäytäntöä (Lohse & Viitanen, 2019, s. 242).

### 2.1.2 Tiedustelun periaatteet

Tiedustelutoimintaa suoritettaessa ja lainsäädäntöä tulkittaessa tulkinnan lopputuloksen on oltava linjassa perus- ja ihmisoikeusnormin kanssa (Lohse & Viitanen, 2019, s. 28). Periaatteet toiminnan harjoittamiselle kaikissa olosuhteissa ovat samat ja tiedustelutoimintaan liittyen onkin määritelty suhteellisuusperiaate, vähimmän haitan periaate ja tarkoitussidonnaisuuden periaate. "Epäeettinen toiminta on aina syvässä ristiriidassa tiedusteluviranomaisten yhteiskunnallisen aseman ja siltä edellytettävän luottamuksen kanssa" (Lohse & Viitanen, 2019, s. 217).

Suhteellisuusperiaatteella viitataan tietyn päämäärän tavoitteluun siten, että käytetyt menetelmät ja niistä aiheutuvat haitat ovat järkevässä suhteessa päämäärään nähden (Lohse & Viitanen, 2019, s. 30). Kaiken henkilökohtaisen datan käsittelyn täytyy perustua johonkin tarkoitukseen ja datan käsittelyn tulee kokonaisuudessaan olla mahdollisimman vähäistä (Akhgar, ym., 2016, s. 291). Tässä asiayhteydessä viitataan erityisesti menetelmiin, jotka puuttuvat yksityiselämän suojaan.

Vähimmän haitan periaatteella tarkoitetaan käytännössä sitä, että toimintatavoista käytetään sitä, joka vähiten puuttuu kohdehenkilön perus- ja ihmisoikeuksiin (Lohse & Viitanen, 2019, s. 32).

Tarkoitussidonnaisuudella viitataan yleisesti siihen, että tiedustelutoiminnan tarkoitus perustuu lainvoimaiseen toimivaltuuteen ja tietyn tehtävän toteuttamiseen (Lohse & Viitanen, 2019, s. 34). Lisäksi tiedustelun periaatteena on syrjinnän kielto, ja periaatteet käskevät formaalisen kriteeristön mukaan toteuttamaan jonkin arvon tai tavoitteen oikeudellisten ja tosiasiallisten reunaehtojen sallimissa rajoissa (Lohse & Viitanen, 2019, s. 244). Vaikka laillinen näkökulma tutkinnan suorittamiselle olisikin, täytyy kuitenkin puntaroida sitä, kuinka tehtävä voidaan suorittaa tarkoituksenmukaisesti ja siten, että yksityisyyttä rikotaan niin vähän kuin mahdollista (Akhgar, ym., 2016, s. 191).

### 2.1.3 Tiedustelulajit

Yleisen jaottelun mukaan OSINT:in lisäksi muita tiedustelulajeja ovat kuvaustiedustelu, geotiedustelu, henkilötiedustelu ja radiosignaalitiedustelu (HE 203/2017). Avointen lähteiden tiedustelua suoritetaan joko yksinään tai jonkin toisen tiedustelulajin tukena. Avointen lähteiden tiedustelua määritellään tarkemmin luvussa 2.2.

Hallituksen esityksen 203/2017 mukaan avointen lähteiden tiedustelu, kuvaustiedustelu ja geotiedustelu eivät vaadi erityistä säädösperustaa, sillä näissä tiedustelulajeissa käytettävät tiedonhankintakeinot eivät loukkaa yksityisyyden suojaa tai luottamuksellisen viestin salaisuutta. Kuvaustiedustelulla (*IMINT, Imagery Intelligence*) tuotetaan strategisen tason tilannekuvan muodostamiseen käytettävää tietoa esimerkiksi elektro-optisilla menetelmillä ja tutkakuvauksella. Geotiedustelulla (*GEOINT, Geospatial Intelligence*) taas tarkoitetaan tiettyjen kohteiden, alueiden, luonnonilmiöiden ja olosuhteiden kuvaamista, arviointia ja

esittämistä. Henkilötiedustelu (*HUMINT, Human Intelligence*) on toimintaa, jossa luodaan henkilökohtaisia suhteita ja siihen liittyy henkilökohtaista kanssakäymistä sekä tietyn kohteen tai henkilön henkilökohtaista havainnointia. Suomessa radiosignaalitiedustelu jaetaan radioaalloilla tapahtuvaan viestitiedusteluun (*COMINT, Communications Intelligence*) ja elektroniseen mittaustiedusteluun (*ELINT, Electronic Intelligence*). COMINT on tiedustelua, jolla tarkkaillaan erilaisia radioaalloilla tapahtuvia tiedonsiirtosignaaleja. ELINT:ia taas käytetään muiden kuin viestisignaalien tiedusteluun, kuten tutkalähetteiden ja navigointisignaalien tiedusteluun. (HE 203/2017.)

### 2.1.4 Tiedustelutoimijat

Toimialat tai toimijat, jotka tiedustelua harjoittavat, voidaan jakaa seuraavasti: tiedustelu kansallisen turvallisuuden ylläpitämiseksi, sotilastiedustelu, siviilitiedustelu (poliisi), yritystiedustelu ja yksityistiedustelu (Prunckun, 2013, s. 5). Toisaalta tiedustelutoimintaa tunnistetaan kaikkiaan kahdeksasta toimialasta: päätöksenteon tukeminen kansallisen turvallisuuden ylläpitämisen yhteydessä, sotilastoiminta, kotimaan turvallisuuspalvelut ja muut viranomaissektorit, kilpailulliset- ja yksityiset turvallisuuspalvelut sekä kyber- ja paikkatietotiedustelutoiminta (James Madison University, 2020).

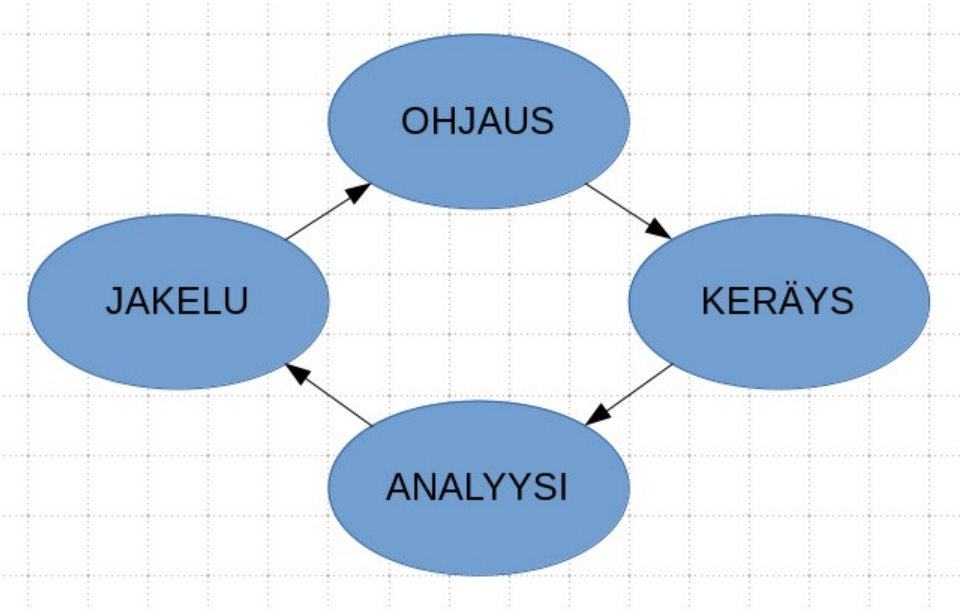
Tiedustelutoimijan perusteella voidaan tehdä joitain oletuksia siitä, millaista tiedustelua kyseisen toimijan toimesta tehdään, ja millaisia kohteita mahdollisesti tiedustelun kohteena on. On myös hyvä huomata, että tiedustelutoimijat ja toimialat usein toimivat päällekkäisesti, sillä esimerkiksi sotilastiedustelun tehtävänä on myös kansallisen turvallisuuden ylläpitäminen. Tässä tutkimuksessa keskityttiin tiedustelulakeihin ja näin ollen tässä tutkimuksessa käsiteltävät tahot ovat Puolustusvoimat ja suojelupoliisi.

### 2.1.5 Tiedusteluprosessi

Tiedustelua kuvataan yleisesti eri lähteissä neljä, tai jopa seitsemän eri vaihetta sisältävänä prosessina, jossa yleisesti tunnetun nelivaiheisen prosessin (ks. kuvio 2) vaiheet ovat toiminnan ohjaaminen, tiedonhankinta, tiedon prosessointi ja analysointi sekä tiedon jakaminen (Lohse & Viitanen, 2019, s. 96). Akhgar ja muut (2016) kuvaavat tiedustelusyklin kuusivaiheisena prosessina, jonka vaiheet ovat ohjaus, keräys, prosessointi, analysointi, jakelu ja palaute (Akhgar, ym., 2016, s. 38).

Käytännössä tiedusteluprosessi käynnistyy tietopyynnöstä *(RFI, Request for Information)* tai tiedustelutehtävän määrittelystä, ja päättyy tiedustelutuotteen jakamiseen tiedon pyytäjälle tai tehtävän antajalle. Prosessin aikana tietoa kerätään ja käsitellään tietyillä menetelmillä ja analysoidaan lopputuotteen valmistamiseksi. Käytännössä tämä kuvaus on hyvin yleismaailmallinen, eikä se kerro kovin konkreettisesti, mitä tiedusteluprosesseissa oikeasti tapahtuu. Tämä kuvaus tiedusteluprosessista kuitenkin auttaa ymmärtämään millaisia toimintoja toimintaan kokonaisuudessaan liittyy. Tiedustelutoiminnassa puhutaan usein

myös tiedusteluympyrästä, jolla mallinnetaan ylempänä kuvattua prosessia, jossa raa'an ja rikastamattoman datan käsittelyn tuloksena tuotetaan valmis tiedustelutuote (Gruszczak, 2016, s. 45).




KUVIO 1 Nelivaiheinen tiedustelusykli (Lohse & Viitanen, 2019, s. 96)

Tiedustelutoiminnan luonnetta voidaan määritellä sen perusteella, kuinka paljon siihen liittyy poliittisia näkökulmia. Silloin, kun tiedustelun päämääränä on tuottaa tietoa poliittisille elimille päätöksenteon tueksi, on vaarana tiedustelun politisoituminen. Tiedustelun politisoitumisella tarkoitetaan sitä, että tiedusteluviranomaisen tiedustelutuote on räätälöity siten, että se tyydyttää tässä tapauksessa poliittista valtaa pitävän asiakkaan näkemyksiä (Lohse & Viitanen, 2019, s. 235).

Tiedustelutoiminnassa keskeisessä roolissa on myös analyysityö, jota analyytikot tekevät tiedustelutuotteen valmistamiseksi. Politisoitumista voi käytännössä tapahtua myös tiedusteluorganisaatioissa, jolloin tiedustelutuote heijastaa analyytikon omia ideologioita tai agendoja (Lohse & Viitanen, 2019, s. 235). Tässä asiayhteydessä voidaan mainita analyytikon työhön liittyviä muita haasteita, joita ovat muun ohella esimiehen ideologian tai agendan myötäily sekä analyytikon ajautuminen omien ajatustensa vangiksi, jolloin tiedustelutuotetta ei voida katsoa objektiivisesti tuotetuksi. Olennainen osa eettistä toimintatapaa on validin ja tarkan tiedon esittäminen.

## 2.2 Avointen lähteiden tiedustelu

Hallituksen esityksessä HE 203/2017 eduskunnalle määritellään avointen lähteiden tiedustelua. Avoimista lähteistä saatavilla oleva tiedustelutieto on tietämystä, joka perustuu avoimista lähteistä kerättyyn informaatioon. Avoimista lähteistä

kerätyn informaation katsotaan koostuvan tiedoista, jotka on mahdollista laillisesti pyytää tai itse havainnoida jokaisen kansalaisen toimesta. Tiedonlähteitä ovat esimerkiksi erilaiset julkaisut ja tilastot, lehdet, kirjallisuus, kartat, sosiaalisen median tiedot sekä yleisölle suunnatut televisio- ja radiolähetykset. Avointen lähteiden tiedusteluun ei kuitenkaan katsota sisältyvän ns. aktiivista osallistumista, jolla tarkoitetaan esimerkiksi avoimessa Internet-verkossa käytävään keskusteluun osallistumista tiedon saamiseksi. Avointen lähteiden tiedustelua voidaan suorittaa omana toimintonaan tai sen tuottamaa tietoa voidaan käyttää jonkin toisen tiedustelutoiminnan tukena. Hallituksen esityksessä HE 203/2017 mainitaan myös se, että avointen lähteiden tiedusteluksi katsotaan yleisesti sellainen toiminta, joka ei loukkaa kohteen yksityisyyden suojaa tai luottamuksellisen viestin salaisuutta. Lisäksi esityksen mukaan avointen lähteiden tiedustelua ei voida määritellä sellaiseksi toiminnaksi, josta perustuslain mukaan olisi säädettävä lailla. (HE 203/2017.)

Bazzell (2019) määrittelee OSINT:ia siten, että se voi tarkoittaa eri asioita eri tahoille. Esimerkiksi CIA:lle (*The Central Intelligence Agency*) OSINT voi tarkoittaa sitä, että tietoa kerätään vieraskielisistä uutislähetyksistä. Asianajajille taas OSINT voi tarkoittaa sitä, että tietoa kerätään hallituksen dokumenteista, jotka ovat julkisesti kaikkien saatavilla. Suurimalle osalle ihmisistä OSINT tarkoittaa kuitenkin sitä, että tietoa haetaan julkisesta Internetistä. Bazzell (2019) on myös nostanut esille Yhdysvaltojen virallisen määritelmän, jonka mukaan OSINT on tietoa, joka on tuotettu julkisesti saatavilla olevasta informaatiosta, joka on kerätty, hyödynnetty ja jaettu tietyssä ajassa, tietyille vastaanottajille ja tiedon tarkoituksena on palvella tiettyä tiedustelun päämäärää. Bazzell myös painottaa sitä, että OSINT-prosessi ei ole vain online-informaation löytämistä, vaan siihen liittyy myös asianmukainen tiedon kerääminen ja raportointi. (Bazzell, 2019, s. 6.)

### 2.2.1 Avoimet lähteet

Nato jakaa avointen lähteiden tiedustelua ja tietoa neljään kategoriaan: avointen lähteiden data, avointen lähteiden informaatio, avointen lähteiden tietous ja validoitu avointen lähteiden tietous, jolla kuvataan datan muuttumista totuuden mukaiseksi tietoudeksi (Akhgar, ym., 2016, s. 70).

Gibsonin (2011) mukaan avoimia lähteitä voidaan karkeasti luokitella kategorioihin: mediat, harmaa kirjallisuus, kaupalliset tuotteet ja ihmislähteet (Gibson, 2011, s. 80).

Akhgarin ja muiden (2016) mukaan avoimiin lähteisiin luetaan harmaat lähteet, joita ovat esimerkiksi artikkelit, raportit, valkoiset kirjat ja muu kirjallisuus, joita ei voida suoranaisesti lukea perinteisiin avoimiin lähteisiin ja niiden löytäminen voi olla myös haastavaa (Akhgar, ym., 2016, s. 81).

Prunckunin (2013) mukaan avointen lähteiden informaatiota voidaan määritellä tarkemmin myös siten, että se sijaitsee joko sisäisessä tai ulkoisessa domainissa. Tällä tarkoitetaan sitä, että sisäinen domain sisältää tietoa, joka sijaitsee jossain organisaation tai toimijan omassa tietokannassa tai arkistossa. Ulkoisella domainilla taas tarkoitetaan tietoa, joka on saatavilla joko avoimesta tai suljetusta

aladomainista (Prunckun, 2013, s. 47). Avoimet domainit käsittävät kaikki perinteiset avoimet tietolähteet, kuten mediat, radiolähetykset ja kaikki muut avoimet tietolähteet. Suljetuilla domaineilla taas viitataan sellaisiin julkisiin lähteisiin, joihin pääsee käsiksi esimerkiksi maksua vastaan, mutta niitä ei silti luokitella salaisiksi. Lisäksi voidaan määritellä muita domaineja, kuten vieraskieliset domainit, joiden hyödyntämisestä voi olla paljonkin etua OSINT-tutkinnassa (Prunckun, 2013, s. 47). Erityisesti maailmanlaajuisen verkottumisen vuoksi avoimista lähteistä saatavilla oleva tietomäärä on loputon ja olennaista ansiokkaan avointen lähteiden tiedustelun toteuttamiseksi onkin se, että ymmärtää mistä tietoa kannattaa etsiä ja millaisilla hakumenetelmillä (Prunckun, 2013, s. 48).

Williamsin ja Blumin mukaan Loch. K. Johnson on esitellyt kirjassaan *Handbook of Intelligence Studies* (2007) erään mallin, jonka mukaan OSIF (*Open Source Information*) ja OSINT voidaan jaotella neljään kategoriaan. Mallin mukaan avointen lähteiden data voidaan jaotella raakatulosteeseen, yleislähetykseen, suulliseen haastattelutietoon ja muuhun informaatioon, joka saadaan primäärilähteestä. OSIF:a taas kyseisessä kirjassa määritellään dataksi, joka saadaan yhdistelemällä geneeristä informaatiota, joka taas on jaettu yleisesti esimerkiksi uutislehtisissä, kirjoissa, radiolähetyksissä ja päivittäisissä raporteissa. OSINT taas määritellään informaatioksi, joka on valikoidulle joukolle prosessoitua tietämystä. Käytännössä siis avoimista lähteistä saatu data ei välttämättä tuo arvoa yksinään, mutta voi sisältää yhdistettynä muuhun dataan merkityksellistä tiedustelutietoa. Tässä asiayhteydessä puhutaan usein myös tiedon rikastamisesta. Williams ja Blum ovat esittäneet myös tästä hyvän esimerkin: yksittäinen *Twitter* -twiitti yksittäiseltä henkilöltä koskien ISIS -järjestön tilaa, ei välttämättä ole vielä merkittävä tiedustelutieto, mutta yhdistettynä tietyn maantieteellisen alueen muihin twiitteihin, voidaan tästä datan yhdistelmästä saada hyvin merkittävääkin tiedustelutietoa (Williams & Blum, 2018, s. 9-10).

### 2.2.2 Sosiaalisen median tiedustelu

Tapaus "Arabikevät" herätteli tiedusteluyhteisöä sosiaalisen median tärkeyden osalta, sillä tapauksessa protestit organisoitiin verkossa ja sosiaalisen median rooli korostui verrattuna perinteiseen tiedusteluun (Liaropoulos, 2013). Sosiaalisen median alustojen käyttäjämäärät ja sosiaalisesta mediasta saatava tietomäärä ovat sen verran valtavia, että onkin perusteltua puhua erikseen sosiaalisen median tiedustelusta. Sosiaalinen media on rajoituksistaan huolimatta yksi työkalu lisää tiedustelutoimijoille sosiaalisen luonteen ymmärtämiseksi ja ennustamiseksi (Liaropoulos, 2013). Tiedustelutoimijat puhuvatkin nykyään sosiaalisen median tiedustelusta (*SOCMINT, Social Media Intelligence*) omana tiedustelulajinaan siihen liittyvien erityisen sisällön ja kompleksisten tekniikoiden vuoksi (Liaropoulos, 2013). Sosiaalisen median tiedustelua voidaan määritellä sosiaalisen median datan tunnistamiseksi ja ymmärtämiseksi OSINT:n ja koneoppimisen keinoin, tavoitteena tunnistaa kansallista turvallisuutta uhkaavaa käytöstä (Şuşnea & Iftene, 2018, s. 231). Sosiaalisen median tiedustelun kohdalla voidaan sen erityispiirteiden vuoksi pohtia SOCMINT:n ja HUMINT:n yhdistämistä

omaksi tiedustelulajikseen, digitaaliseksi henkilötiedusteluksi (DIGITAL HUMINT) (Lombardi, Rosenblum & Burato, 2015, s. 4).

Sosiaalisen median rooli tiedonhankinnan lähteenä on viime vuosina korostunut esimerkiksi terrorismin ja protestien vuoksi. Näiden tapahtumien esiintyminen voidaan tunnistaa paljon nopeammin analysoimalla sosiaalisia verkostoja, kuin perinteisiä uutislähteitä analysoimalla (Şuşnea & Iftene, 2018, s. 232). Yksi keskeinen ongelma sosiaalisen median datan analysoinnissa on datan valtava määrä, josta käytetään nimitystä *Big Data*. Sosiaalisen median datan analysoinnissa korostuukin datanlouhintatekniikoiden tehokas käyttö (Şuşnea & Iftene, 2018, s. 232). Sosiaalisen median alustoista *Twitter* nähdään usein monipuolisimpana tietolähteenä, sillä sen käyttäjäkunta on laaja sekä maantieteellisesti, että statuksellisesti. *Twitterissä* esiintyvät julkaisut vaihtelevat poliitikkojen kannanotoista tavallisten kansalaisten mielipiteisiin.

### 2.2.3 Avointen lähteiden tiedustelun tekniikat lyhyesti

Yksi merkittävä tekijä informaatiomäärän kasvuun ja ihmisten verkottumiseen on ollut matkapuhelin, joka mahdollistaa tiedon tuottamisen jatkuvasti ja lähes mistä tahansa. Seuraavana vastaavanlaisena informaatiomäärän paisuttajana nähdään Esineiden Internet (engl. *The Internet of Things*) tai Kaiken Internet (engl. *The Internet of Everything*), joka jälleen lisää verkottumista (Omand, 2015, s. 9).

Internet-tiedustelussa käytettäviä työkaluja, tekniikoita sekä menetelmiä on lukuisia ja niitä voidaan käyttää eri tilanteisiin (ks. kuvio 2). Työkalut myös päivittyvät jatkuvasti ja uusia työkaluja ilmestyy jatkuvasti lisää, joten käytettävät työkalut ja tekniikat myös vanhentuvat nopeasti. Internet voidaan OSINT:n näkökulmasta jakaa näkyvään verkkoon ja *darknet*-verkostoon. On arvioitu, että Internetin sisällöstä 80 – 90 % on indeksoimatonta sisältöä (Akhgar, ym., 2016, s. 82). Tästä Internetin osasta käytetään usein nimitystä *Deep Web*. Tämän lisäksi voidaan puhua vielä *Dark Webistä*, jolla tarkoitetaan sellaista *Deep Webin* osaa, johon käsiksi pääseminen vaatii tiettyä selainta, kuten *Tor*-selainta tai tiettyä käyttöjärjestelmää, kuten *Tailsia* (Akhgar, ym., 2016, s. 82). *Dark Webiin* kuuluu useita erillisiä *darknet*-verkkoja, joita ovat esimerkiksi *Tor (the Onion Router)*, *I2P (Invisible Internet Project)* ja *Freenet* (Akhgar, ym., 2016, s. 114).

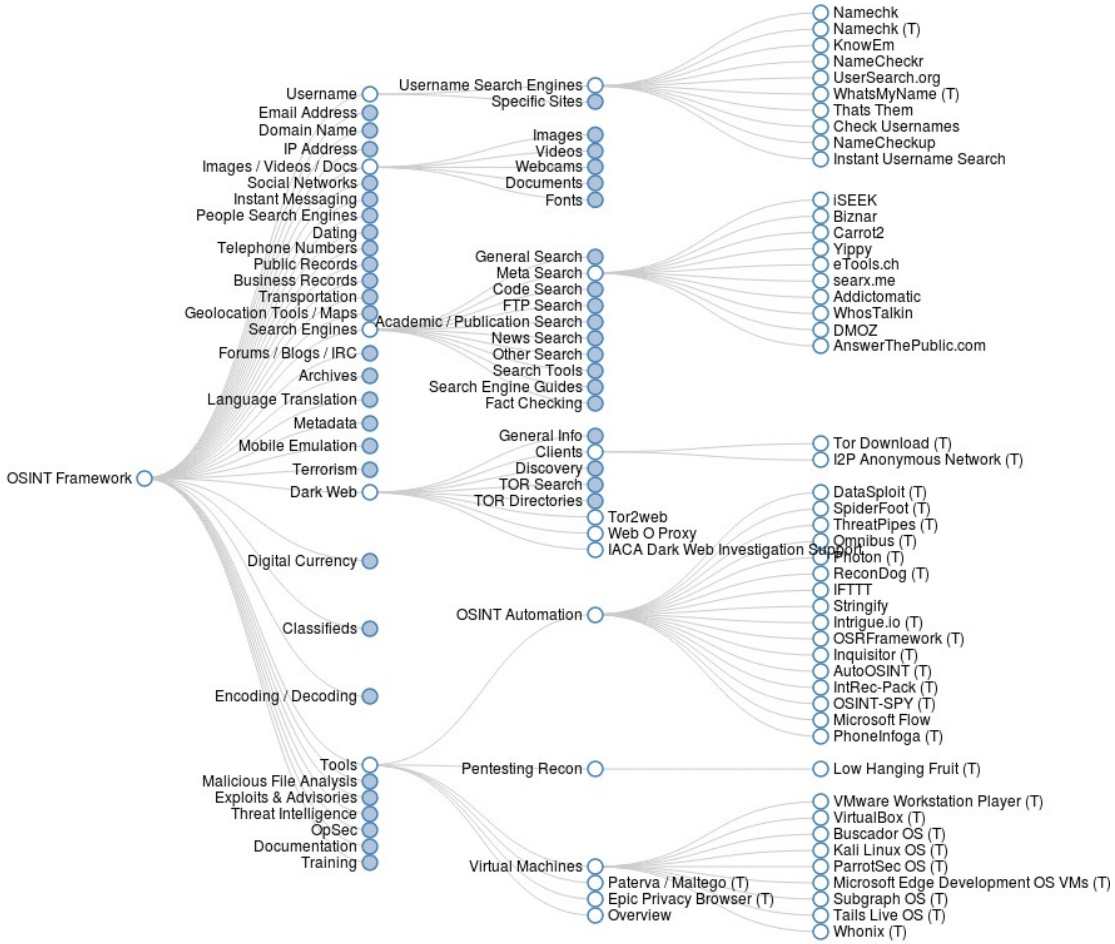
KUVIO 2 Havainnollistava kuva OSINT-menetelmien laajuudesta (Bellingcat's Online Investigation Toolkit, 2020)

Bazzellin (2019) mukaan tietojen tallennus- ja keräysmenetelmät voidaan jakaa kolmeen kategoriaan. Keräysmenetelmät ovat: manuaalinen keräys, passiivinen keräys ja skriptattu keräys. Manuaalisella tietojen keräyksellä tarkoitetaan tietojen keräämistä ja tallentamista käyttäjälähtöisesti. Passiivinen tietojen keräys ja tallentaminen taas tarkoittavat sitä, että tietoja tallennetaan ja kerätään passiivisesti työkalun toimesta lähdekoodin tasolla, mukaan lukien sivustojen sisältämät kuvat. *Hunchly* -niminen passiivinen tietojen keräystyökalu on paras esimerkki tästä. Skriptatulla keräysmenetelmällä tarkoitetaan sitä, että manuaalisesti aktivoidut ohjelmat louhivat digitaalista sisältöä kerääjän puolesta. (Bazzell, 2019, s. 516-518.)

Internet-tiedustelun yhtenä tekniikkana voidaan käyttää "*web crawleria*" tai "*spideria*", joka seuraa linkkejä sattumanvaraisesti tai tietyillä ennakkoon asetetuilla reunaehdoilla automaattisesti löytääkseen halutun tiedon (Akhgar, ym., 2016, s. 74). Työkaluja ovat myös esimerkiksi selainten laajennukset, online-palvelut, lähdetietokannat ja asennetut sovellukset (Akhgar, ym., 2016, s. 153). Internet-tiedustelussa hyödyllinen tekniikka on myös RSS:n (*Really Simple Syndication*) käyttö, jolla voidaan seurata esimerkiksi tiettyä aihetta tai blogia automaattisesti (Akhgar, ym., 2016, s. 81). Sosiaalisen median hyödyntämisestä OSINT :ssa käydään paljon keskusteluja, mutta sen merkittävyyttä ei voida mitenkään kiistää. Sosiaalisen median datan keräämiseen voidaan hyödyntää esimerkiksi API-avaimia tai vaihtoehtoisesti havainnoida manuaalisesti itse. Yksi yleisimmistä datanhankintakeinoista onkin API:n (*Application Programming Interface*) hyödyntäminen. (Akhgar, ym., 2016, s. 76).

Tekniikoista löytyy esimerkiksi *GitHubista* valmiita listoja, joihin on kerätty kattavasti erilaisia työkaluja. Olemassa on paljon erilaisia listoja ja kokoelmia, mutta jokaisen täytyy kuitenkin tutkia mitä itse toiminnassaan tarvitsee, eikä mitään absoluuttista vastausta ole valmiiksi olemassa. Lisäksi myös esimerkiksi

sivustolta *osintframework.com* saa käsitystä siitä, miten tietoa etsitään (ks. kuvio 3).




KUVIO 3 OSINT Framework -sivuston esimerkkinäkymä (OSINT Framework, n.d.)

Aina Internet-sivustoilla vierailtaessa jää toiminnasta jälki, joten tätä tulisi pohtia Internet-tiedustelua suoritettaessa. Lisäksi tässä asiayhteydessä tulisi pohtia myös toiminnan dokumentointia, jolloin on olemassa kirjanpito tehdyistä toimista tutkinnan aikana (Akhgar, ym., 2016, s. 286). Tämä pohdinta koskee erityisesti viranomaispuolta ja erityisesti sellaisia tehtäviä, joissa todistusaineistoa käytetään mahdollisesti oikeudellisissa tarkoituksissa. Toiminnan dokumentointi voidaan kuitenkin katsoa myös eettiseksi toimintatavaksi, sillä dokumentoinnin yhteydessä joudutaan väkisinkin samalla pohtimaan toiminnan syitä ja perusteita. Internet-tiedustelussa kannattaa huomioida myös se, että esimerkiksi hakukoneet, kuten *Google*, tallentavat tarkkoja tietoja tehdyistä hauista profilointia varten ja sivustojen omistajat pystyvät usein jäljittämään vierailijansa (Johnson, 2013, s. 216). Tämän lisäksi sivustot myös raportoivat eteenpäin siitä, mitä vierailijat muilla sivustoille tekevät (Johnson, 2013, s. 216).

On myös hyvä huomata, että vaikka avoimista lähteistä kerätyt tiedot olisivatkin julkisia, on tiedonkeräysprosessissa usein sellaisia komponentteja, jotka halutaan salata. Esimerkiksi tiedonkerääjän henkilöllisyys,

tiedonkeräystekniikat ja operaation kokonaiskuva, kuten tiedonkeräyksen tarkoitus, ovat usein salassa pidettäviä tietoja (Gibson, 2011, s. 81).

### 2.2.4 Tietojen analysointi ja käytettävyys

*Twitteristä* voidaan usein löytää tietoja kohteen mielipiteistä ja ideologiasta, *Facebookista* ja *LinkedIn:stä* taas tunnistetaan sosiaalisia verkostoja ja henkilökohtaisempia tietoja (Prunckun, 2013, s. 55). *Facebookista* voidaan joissain tapauksissa päätellä tarkastikin kohteena olevan henkilön koko sosiaalinen verkosto, lähimmät ystävät, parhaimmat työkaverit, sisarukset, sukulaiset, muut tuttavat, harrastukset ja niin edelleen. *LinkedIn:stä* taas voidaan saada viitteitä kohteen varallisuustasosta, työhistoriasta, kollegoista, asemasta ja taidoista (Prunckun, 2013, s. 55).

Erityisesti silloin, kun tiedustelun kohteena on henkilö, päästään läheisesti kiinni käsitteeseen tiedon rikastaminen tai *"Mosaic Effect"*. Mosaiikki vaikutus (engl. *Mosaic effect*) kuvaa sitä, miten pienistä palasista voi muodostua jokin merkityksellinen suurempi kokonaisuus. Termi on tuttu tiedustelun kontekstissa ja konkreettisesti sillä tarkoitetaan sitä, että yksittäiset joskus merkityksettömiltä vaikuttavat tiedon osaset muodostavat yhdessä jonkin merkityksellisen ja arvokkaan kokonaisuuden. Tiedonkeräystä suoritettaessa saatetaan löytää yksittäisiä tietoja eri paikoista, mutta tiedot yksinään eivät vielä välttämättä kerro tiedon kerääjälle paljoakaan. Yksittäisiä tietoja analyytikon toimesta yhdistelemällä voidaan kuitenkin saada aikaan laajempia kokonaisuuksia, jotka ovat tiedon kerääjälle tärkeitä.

Avoimet lähteet tarjoavat mahdollisuuksia tiedustelutoimijalle, mutta kaikilla muillakin on pääsy samoihin lähteisiin. Tiedustelun kohteena oleva taho saattaa esimerkiksi yrittää väärentää julkisia tietoja tai ohjata tiedonkerääjiä harhaan, jos kohde epäilee olevansa tiedustelun kohteena (Akhgar, ym., 2016, s. 88). Virheellisen tiedon levittämiseen voi olla myös useita muita syitä. Internetin käyttäjät saattavat tahattomasti jakaa virheellistä tietoa, sillä käyttäjät saattavat tulkita itse virheelliset tiedot oikeiksi. Internetin käyttäjät saattavat myös olla huolissaan yksityisyydestään ja tämän oletuksen pohjalta muuttaa julkisia tietojaan (Akhgar, ym., 2016, s. 88).

Avoimista lähteistä saatujen tietojen tarkkuuden ja oikeellisuuden arviointiin voidaan käyttää erilaisia taulukkoja, asteikkoja ja arviointeja. Esimerkiksi Yhdysvaltojen armeija ja Nato käyttävät kuusiportaista asteikkoa: ei epäilystä luotettavuudesta, luotettava, historian perusteella täysin luotettava, puuttuu luotettavuus, epäluotettava ja historian perusteella epäluotettava (Akhgar, ym., 2016, s. 107). Nato:lla on lisäksi olemassa muita kriteerejä autenttisuuden arviointiin. Arvioitavia kriteerejä muun ohella ovat kuka sisällöstä vastaa, kieliasun tarkastelu, mikä sisällön tavoitteena on, sisällön julkaisun päivämäärät ja kuinka laajamittaista sisältö on (Akhgar, ym., 2016, s. 107).

### 2.2.5 Etiikka ja toimintatavat

Sosiaalisen median ja henkilötietojen käytöstä osana tutkintatarkoitusta käydään usein kiivasta keskustelua, jonka vuoksi organisaatioiden sisällä tulisi olla kyseisistä aiheista selkeä linjaus (Bazzell, 2019, s. 555). Bazzell (2019) on esittänyt, että ristiriitatilanteiden välttämiseksi olisi hyvä olla olemassa lyhyt asiakirja tai dokumentti, joka määrittelisi OSINT-tutkinnan asianmukaisia toimintatapoja (Bazzell, 2019, s. 555). Tiedustelutuotteen uskottavuus rakentuu kykyyn tuottaa eettistä ja tarkkaa tietoa (Prunckun, 2013, s. 61).

Ihmislähtöiset arvot ja periaatteet ohjaavat tekemisiämme siten, että arvoja ja periaatteita kunnioittamalla saavutetaan toiminnan taso, jota voidaan kutsua hyväksi tiedustelutavaksi (Lohse & Viitanen, 2019, s. 217). Hyvät tiedustelutavat toisin sanoen rakentuvat moraalisen kompassin ja eettisten toimintatapojen ympärille ja sen teoreettiseksi perustaksi on esitetty oikeutettua sodankäynnin teoriaa (engl. *JWT – Just War Theory*) (Lohse & Viitanen, 2019, s. 217). Oikeutetun sodankäynnin teorian perusperiaatteet on tiivistetty seuraavasti: oikeutettu syy, viimeinen keino, asianmukaisen tahon julistama, oikeat aikomukset, kohtuulliset mahdollisuudet menestykseen ja hyväksyttävästi suhteutetut keinot (Moseley, n.d). Tiedustelun eettisyyttä ja hyviä toimintatapoja voidaan välillisesti edistää myös ns. *Whistleblower*-järjestelmän avulla, jonka avulla epäeettisyydestä ja laittomasta toiminnasta olisi mahdollista ilmoittaa ilmoittajan suojasta ja nimettömyydestä nauttien (Lohse & Viitanen, 2019, s. 233).

Yksi mielenkiintoinen pohdinnan aihe liittyy avointen lähteiden Internet-tiedustelussa rajat ylittävään toimintaan. On käytännössä lähes mahdotonta suorittaa tiedustelua siten, että toiminta rajautuisi vain tiettyyn maahan, sillä maailma on niin vahvasti verkottunut. Avointen lähteiden Internet-tiedustelua voidaankin kutsua tiedustelutoiminnaksi rajattomassa ympäristössä (Akhgar, ym., 2016, s. 287). Tähän rajattomaan toimintaan maantieteellisessä merkityksessä liittyy haasteita lainsäädännöllisestä näkökulmasta, sillä maiden kansalliset lainsäädännöt eroavat toisistaan ja tietojen hankkimiseen joidenkin maiden välillä liittyy tiettyjä haasteita (Akhgar, ym., 2016, s. 287).

Bazzell (2019) käsittelee *Open Source Intelligence Techniques* –kirjassaan OSINT-toimintaan liittyviä hyviä toimintatapoja ja eettisiä näkökulmia. Hänen mielestään tulisi välttää sitä, että toimintatapoja sidotaan tiettyihin menetelmiin, alustoihin ja teknologioihin, sillä teknologinen kehitys on nopeaa. Nopean kehityksen seurauksena tiettyihin menetelmiin, alustoihin ja teknologioihin sidotut toimintatavat ovat tehottomia ja usein hyvinkin nopeasti irrelevantteja. Tämän seurauksena myös voidaan joutua tekemään hankalia päätöksiä toiminnan toteuttamisen suhteen, joka ei palvele lainkaan tehtävien suorittamista. Toimintatavat tulisikin vahvasti sitoa siihen, kuinka erilaisia tekniikoita ja teknologioita käytetään asianmukaisesti. Asianmukaisen käytön määritelmän voi esimerkiksi sitoa organisaation jo olemassa oleviin käytänteisiin. Bazzellin (2019) mukaan on tärkeää, että OSINT-toimintaan liittyvät toimintatavat on dokumentoitu, jolloin toiminnan toteutusta voidaan tarvittaessa perustella dokumenttien avulla. Organisaation toimintatapojen dokumentointi voidaan usein jakaa kahteen osaan.

Organisaatiolla voi olla ns. virallinen toimintataparakenne ja sen lisäksi voi vielä erikseen olla ns. yleisten operointimenetelmien kokoelma (engl. *Set of Standard Operating Procedures – SOPs*) (Bazzell, 2019, s. 555-558).

Internetissä on paljon kaikkien saatavilla olevaa julkista tietoa, mutta lisäksi on olemassa kaikkien laillisesti saatavilla olevaa kyseenalaista tietoa. Tällaista tietoa voisi olla esimerkiksi väärin konfiguroidun *Elasticsearch* -tietokannan tieto, johon päästään käsiksi selaimella syöttämättä mitään kirjautumistietoja. Tällaisessa tilanteessa kuitenkin hyödynnetään toisen osapuolen virhettä, eikä toinen osapuoli ole tarkoituksella jakanut tietoja, joihin päästään käsiksi. Bazzellin (2019) mukaan tällaisissa tilanteissa tiedonkerääjän aikomukset ja motiivit määrittelevät sen, onko tietojen hyödyntäminen asianmukaista vai ei. Kuvitellaan sellainen tutkinta, jossa epäillään lapsiin kohdistuvaa rikosta. Tällaisessa tutkinnassa tiedonkerääjän motiivi kyseenalaisten tietojen keräämiselle on hyvin perusteltu. Tiedonkeräyksessä halutaan aina tasapainoilla vaikutuksella henkilöiden yksityisyyteen ja yhteisen hyvän periaatteen välillä. (Bazzell, 2019, s. 559-560.)

Eettisyyden ja lainsäädännön näkökulmasta yksityisyyteen liittyvät asiat esiintyvät vahvasti avointen lähteiden Internet-tiedustelun kontekstissa. Bazzell (2019) painottaa sitä, että jokainen OSINT-tehtävä on erilainen ja jokaisen tehtävän osalta tulisi aina arvioida tarkasti sitä, kuinka pitkälle tiedonkeräyksessä mennään (Bazzell, 2019, s. 559). Jos tehtävä voidaan suorittaa yhden kuvankaappauksen perusteella, ei ole syytä tutkia asiaa sen pidemmälle. Avointen lähteiden tiedustelun tietoja käytetään jossain toiminnassa myös todistusaineistona oikeudessa asti, joten datan keräyksen tulee olla oikeutettua ja dataa ei tule kerätä enempää kuin tosiasiallisesti on tarvetta (Akhgar, ym., 2016, s. 69).

Kaikissa OSINT-tapauksissa ei ole mahdollista tarkasti määritellä tehtävään liittyviä yksityiskohtia. Jos OSINT:n tarkoituksena on tutkia tiettyä henkilöä, tulisi kuitenkin kyetä tunnistamaan tutkinnan oikeuttavia asianhaaroja, sillä tutkinnassa tutkitaan tietyn henkilön elämää. Bazzell (2019) kuvailee asiaa siten, että ”en seuraa tuntematonta henkilöä kadulla, joten osoitan harkintaa myös niissä tilanteissa, joissa aion suorittaa tutkintatyötä Internetissä” (Bazzell, 2019, s. 560).

# 3 TUTKIMUKSEN TOTEUTUS

Tässä luvussa kuvataan tutkimuksen toteutus, johon liittyy tutkimusaineiston esittely, tutkimusmenetelmä ja tutkimusprosessin kuvaus. Tutkimuksessa käytetään kvalitatiivista tutkimusotetta ja tutkimusmetodina käytetään aineistolähtöistä sisällönanalyysia. Tutkimuksessa on vaikutteita grounded theory -tutkimussuuntauksesta.

## 3.1 Tutkimuksen aineisto

Tutkimuksen tutkimusaineisto koostuu sotilas- ja siviilitiedustelulaeista. Tutkimuksen aineistoon lasketaan mukaan myös näiden lakien taustalla olevat esityöt, jotka ovat löydettävissä eduskunnan sivustolta. Lakien esitöistä tarkasteluun on otettu asian käsittelytietojen keskeiset asiakirjat. Yksityiskohtainen tutkimusaineiston määrittely esitetään alempana. Lakien valmisteluasiakirjat koostuvat komiteanmietinnöistä, työryhmäraporteista, hallituksen esityksistä ja eduskunnan valiokuntamietinnöistä, joista käy parhaiten ilmi lainsäätäjän tarkoitus (Eduskunta, n.d.).

### 3.1.1 Sotilastiedustelulaki

Aineiston ensimmäinen osio koostuu sotilastiedustelulaista (Laki sotilastiedustelusta 590/2019) ja siihen liittyvistä esitöistä. Esitöillä tarkoitetaan asian käsittelytietoja (HE 203/2017 vp) asiassa hallituksen esitys eduskunnalle laiksi sotilastiedustelusta sekä eräiksi siihen liittyviksi laeiksi. Käsittelytiedoista on tähän aineistoon otettu keskeiset asiakirjat, jotka on eritelty alempana:

- Vireilletuloasiakirja, HE 203/2017 vp
- Valiokunta-asiakirja, TrVL 4/2018 vp
- Valiokunta-asiakirja, UaVL 6/2018 vp
- Valiokunta-asiakirja, LiVL 27/2018 vp
- Valiokunta-asiakirja, PeVL 36/2018 vp
- Valiokunta-asiakirja, HaVL 42/2018 vp
- Valiokunta-asiakirja, LaVL 31/2018 vp
- Valiokunta-asiakirja, PuVM 4/2018 vp
- Valiokunta-asiakirja, PeVL 76/2018 vp
- Valiokunta-asiakirja, PuVM 9/2018 vp
- Eduskunnan vastaus, EV 290/2018 vp
- Valiokuntien asiantuntijalausunnot (213). (Eduskunta, 2020.)

### 3.1.2 Siviilitiedustelulaki

Aineiston toinen osio koostuu siviilitiedustelulaista (Poliisilaki 5 a luku 26.4.2019/581) ja siihen liittyvistä esitöistä. Esitöillä tarkoitetaan asian käsittelytietoja (HE 202/2017 vp) asiassa hallituksen esitys eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi. Käsittelytiedoista on tähän aineistoon otettu keskeiset asiakirjat, jotka on eritelty alempana:

- Vireilletuloasiakirja, HE 202/2017 vp
- Valiokunta-asiakirja, TrVL 3/2018 vp
- Valiokunta-asiakirja, UaVL 5/2018 vp
- Valiokunta-asiakirja, LiVL 26/2018 vp
- Valiokunta-asiakirja, PuVL 16/2018 vp
- Valiokunta-asiakirja, PeVL 35/2018 vp
- Valiokunta-asiakirja, LaVL 32/2018 vp
- Valiokunta-asiakirja, HaVM 30/2018 vp
- Valiokunta-asiakirja, PeVL 75/2018 vp
- Valiokunta-asiakirja, HaVM 36/2018 vp
- Eduskunnan vastaus, EV 291/2018 vp
- Valiokuntien asiantuntijalausunnot (254). (Eduskunta, 2020.)

## 3.2 Kvalitatiivinen tutkimus

Tässä tutkimuksessa käytetään kvalitatiivista eli laadullista tutkimusotetta. Laadullisen tutkimuksen ominaispiirteenä voidaan pitää sitä, että tutkittavaa kohdetta tutkitaan mahdollisimman kokonaisvaltaisesti ja lähtökohtana voidaan pitää todellisen elämän kuvaamista (Hirsjärvi, Remes & Sajavaara, 2004, s. 152). Hirsjärven, Remeksen ja Sajavaaran (2004) mukaan laadullisessa tutkimuksessa on ominaista myös se, että tutkimuksessa käytetään induktiivista analyysia, jonka mukaan lähtökohtana on tutkimusaineiston yksityiskohtainen tarkastelu. Tuomen ja Sarajärven mukaan Töttö (2000) kärjistää laadullista tutkimusta tutkimukseksi ja analyysiksi, josta on jätetty pois kaikki numeroaineistot ja tilastolliset menetelmät (Tuomi & Sarajärvi, 2018, s. 19).

Teoria on käsitteenä haastava, mutta Tuomen ja Sarajärven (2018) mukaan havaintojen teoriapitoisuus on yksi laadullisen tutkimuksen peruskulmakivistä, johon tutkimuksen perusteluissa nojataan. Heidän mukaansa havaintojen teoriapitoisuus tarkoittaa sitä, että tutkimuksen tuloksiin vaikuttaa se, millaisia välineitä tutkimuksessa käytetään, millainen käsitys ilmiöstä on ja mitä merkityksiä tutkittavalle ilmiölle annetaan. Puhtaasta objektiivisesta tiedosta ei voida tutkimuksessa puhua, vaan tutkija päättää tutkimusasetelmasta oman ymmärryksensä varassa, jolloin kaikki tieto on tässä mielessä subjektiivista. Tutkimuksen teoria on Tuomen ja Sarajärven (2018) mukaan oikeastaan tutkimuksen viitekehys, mutta teoriaa tarvitaan myös koko tutkimuskokonaisuuden, kuten

metodien ja luotettavuuden hahmottamiseen. Viitekehys jakaantuu käsitteellisenä ilmiönä kahteen osioon, jotka ovat tutkimusta ohjaava metodologia ja jo tutkittavasta ilmiöstä tiedossa olevat asiat. Tämä viitekehyksen jako ei välttämättä palvele tutkimuksen toteuttamista, mutta se riittää määrittelemään teoriaa laadullisessa tutkimuksessa. (Tuomi & Sarajärvi, 2018, s. 18-19.)

Laadullisesta tutkimuksesta tunnistetaan useita tutkimussuuntauksia, joita ovat muun ohella fenomenografia, grounded theory -lähestymistapa, etnografia, toimintatutkimus, tapaustutkimus ja sosiaalinen konstruktionismi. Fenomenografiassa keskitytään käsitysten eroavaisuuksien tutkimiseen, jossa pääpainona on tutkia ihmisten erilaisia käsityksiä tutkittavasta ilmiöstä. Grounded theory on metodologinen viitekehys, jota käytetään perinteisesti uuden tai vähän tutkitun ilmiön tutkimiseen. Metodologia on aineistolähtöinen ja sen avulla pyritään muodostamaan uutta teoriaa sekä selvittämään ilmiön perustaa. Etnografiassa taas tutkija osallistuu tutkimuksen piirissä elävien ihmisten arkeen ja pyrkii siten tarkastelemaan ja ymmärtämään tutkittavaa kohdetta. Toimintatutkimuksen tavoitteena on sekä tutkia, että yrittää muuttaa vallitsevia käytänteitä. Tutkimukselle on tyypillistä, että tutkittavat ovat aktiivisesti osana tutkimusta. Tapaustutkimuksessa nimensä mukaisesti tutkitaan tiettyä tapausta tai tapauksia. Tavoitteena on pyrkiä tutkimaan ja selittämään tapauksia miten- ja miksi-kysymysten avulla. Sosiaalinen konstruktionismi on tutkimussuuntaus, jonka mukaan todellisuus rakentuu kielellisen vuorovaikutuksen ympärille. (Saaranen-Kauppinen & Puusniekka, 2006.)

Tutkimussuuntauksista tässä tutkimuksessa on otettu vaikutteita grounded theory -lähestymistavasta. Tässä tutkimuksessa tutkitaan tiettyä aineistoa ja tavoitteena on löytää, mitä aineistossa sanotaan avointen lähteiden tiedusteluun liittyen. Grounded theory (GT) -lähestymistavan perustana on se, että tutkittavaa kohdetta ei ole aiemmin tutkittu tai siitä on vain vähän tutkittua tietoa sekä tutkimuksen lähtökohtana on aineistolähtöisyys. Myös nämä GT:ta kuvaavat erityispiirteet ovat erotettavissa tämän tutkimuksen asettelusta. GT:ssä aineiston analyysin perustana käytetään luokittelua, joka on myös tämän tutkimuksen analyysimenetelmän perusta. Tässä luvussa esiteltyjen muiden tutkimussuuntauksien osalta ei voida löytää selkeitä yhteyksiä tähän tutkimukseen.

GT on saanut tutkijoiden toimesta erilaisia tulkintoja ja painotuksia, mutta GT:n perusajatus on aineiston analysoiminen empiriaa painottaen ja teorian muodostaminen aineiston luokittelun ja vertailemisen johdolla. Straussin ja Corbinin (1990) mukaan teoriaa muodostetaan aineistosta systemaattisesti koodaten ja luokitellen. GT:n yhteydessä puhutaan myös tyypillisesti saturaatiosta, eli aineistoa kerätään niin kauan, kunnes uusi aineisto ei enää tuo lisäarvoa teorian muodostukseen. (Saaranen-Kauppinen & Puusniekka, 2006.) Tässä tutkimuksessa aineistoa ei kuitenkaan enää kerätä tutkimuksen edetessä lisää, vaan tutkimusaineisto on ennalta määritetty. Tutkimuksessa on otettu vaikutteita GT:stä tutkimussuuntauksena, mutta GT:n perusajatuksia ei kokonaisuudessaan tässä tutkimuksessa sovelleta. Tässä tutkimuksessa ei esimerkiksi pyritä teorian muodostukseen, vaan sisällönanalyysiin tietystä ennalta määrätystä aineistosta. Aineistoa ei myöskään kerätä lisää tutkimuksen edetessä, vaan tutkittava aineisto

on ennalta määritetty. Ei voida myöskään ennalta tietää, kuinka tyydyttäviä vastauksia tutkimusaineistosta saadaan.

## 3.3 Tutkimusmenetelmä

Tutkimuksen tutkimusmetodina käytetään aineistolähtöistä sisällönanalyysiä. Sisällönanalyysi on perusanalyysimenetelmä, jota voi pitää yksittäisenä metodina (Tuomi & Sarajärvi, 2018, s. 78). Sisällönanalyysi kuuluu sellaiseen laadullisen tutkimuksen analyysiryhmään, jossa analyysia ei ohjaa mikään teoreettinen asemointi (Tuomi & Sarajärvi, 2018, s. 78).

Sisällönanalyysin menetelmällä voidaan systemaattisesti ja objektiivisesti analysoida käytännössä mitä tahansa dokumentteja, joita ovat miltei mitkä tahansa kirjallisessa muodossa olevat materiaalit (Tuomi & Sarajärvi, 2018, s. 87). Sisällönanalyysi valitaan tutkimuksen menetelmäksi, koska sen perusteella voidaan analysoida käytännössä mitä tahansa kirjallisessa muodossa olevaa aineistoa. Tutkimuksen aineisto on selkeästi määritetty ja tutkimuksen tavoitteena on selvittää mitä aineistossa sanotaan avointen lähteiden tiedusteluun liittyen ja sisällönanalyysi sopii tähän tarkoitukseen hyvin. Sisällönanalyysillä saadaan aineistosta selville juuri ne kohdat, joita tutkimusongelmaan vastaamiseksi tarvitaan. Aineisto on jo olemassa, joten tutkimuksessa ei tarvita haastatteluja tai havainnointia. Sisällönanalyysi on myös menetelmänä suoraviivainen ja se palvelee tutkimustehtävän toteuttamista. Tutkimuksen tavoite on myös selkeästi määritetty, joka ohjaa aineiston analyysia. Sisällönanalyysi on myös analyysimenetelmänä joustava, joka perustelee menetelmän käyttöä. Alempana kerrotaan tarkemmin analyysin toteuttamisesta, jonka mukaan analyysissa tehtävää luokittelua voidaan jatkaa niin kauan, kuin se aineiston perusteella on mahdollista tai mielekästä. Tämä perustelee menetelmän käyttöä, koska aineistoa ei ole aiemmin tästä näkökulmasta tarkasteltu, joten myöskään aineiston sisällöstä ei voida tehdä merkittäviä ennakko-oletuksia.

Tuomen ja Sarajärven (2018) mukaan Miles ja Huberman (1994) kuvaavat aineistolähtöistä laadullista eli induktiivista aineiston analyysiä seuraavasti: se on karkeasti kolmivaiheinen prosessi, jossa aineistoa pelkistetään, ryhmitellään ja luodaan teoreettisia käsitteitä eli abstrahoidaan (Tuomi & Sarajärvi, 2018, s. 91). Ennen analysointia on olennaista määrittää analyysiyksikkö, joka voi olla esimerkiksi ajatuskokonaisuus, jonka määrittämistä ohjaa tutkimustehtävä (Tuomi & Sarajärvi, 2018, s. 91).

Tuomen ja Sarajärven (2018) mukaan Lähdesmäki, Oinonen, Sandgren ja Sarajärvi (2000) määrittelevät sisällönanalyysin ensimmäistä vaihetta siten, että tavoitteena on aineiston redusointi eli pelkistäminen siten, että siitä karsitaan tutkimuksen kannalta pois epäolennaiset asiat. Heidän mukaansa tavoitteena on myös löytää aineistosta tutkimustehtävää kuvaavia alkuperäisilmaisuja ja niitä kuvaavia pelkistettyjä ilmauksia. Huomionarvioista tässä on se, että aineistosta voidaan erottaa myös useita pelkistettyjä ilmaisuja, jotka kaikki kuvaavat samaa

alkuperäisilmaisua. Tällä ilmaisujen etsimisellä luodaan myös pohjaa analyysin seuraavalle vaiheelle. (Tuomi & Sarajärvi, 2018, s. 92.)

Analyysin toisessa vaiheessa Tuomen ja Sarajärven (2018) mukaan aineistoa klusteroidaan eli ryhmitellään. Käytännössä tällä tarkoitetaan sitä, että redusoinnin tuloksena saadut alkuperäisilmaukset käydään läpi ja aineistosta etsitään samankaltaisuuksia ja eroavaisuuksia kuvaavia käsitteitä. Samaa ilmiötä kuvaavat käsitteet ryhmitellään luokkiin, joita kutsutaan alaluokiksi. Klusteroinnin tarkoituksena on tiivistää aineistoa, sillä yksittäisiä tekijöitä yhdistellään yleisempiin käsitteisiin. Luokittelua voidaan jatkaa siihen asti, että aineistosta nousee yhdistävä luokka. Alaluokat voidaan yhdistää yläluokiksi, yläluokat pääluokiksi ja lopulta pääluokat yhdistäväksi luokaksi, joka on yhteydessä tutkimustehtävään. (Tuomi & Sarajärvi, 2018, s. 92.)

Aineiston klusteroinnin jälkeen analyysissa edetään Tuomen ja Sarajärven (2018) mukaan käsitteellistämiseen eli abstrahointiin. Käsitteellistämisen tavoitteena on löytää aineistosta olennainen tieto tutkimuksen kannalta. Käsitteellistämistä jatketaan niin kauan, kuin on mahdollista aineiston sisällön perusteella. Käsitteellistäminen on prosessi, jossa tutkija rakentaa kuvausta tutkimuskohteesta käsitteiden avulla. Analyysin tuloksena saadaan aineistosta muodostettuja käsitteitä ja teemoja. Tuomi ja Sarajärvi (2018) myös toteavat, että sisällönanalyysille on olemassa useita variaatioita, eikä aineistolähtöisyyden takia voida etukäteen määrittää, kuinka monta ja mitä luokkia analyysin tuloksena saadaan muodostettua. Luokkien määrä ja niiden suhteet selviävät vasta analyysin edetessä. (Tuomi & Sarajärvi, 2018, s. 94.)

Aineistolähtöisen sisällönanalyysin tuloksena esitetään aineistosta muodostettu malli, käsitejärjestelmä, käsitteet tai aineistoa kuvaavat teemat sekä luokittelujen pohjalta muodostetut käsitteet, kategoriat ja niiden sisällöt. Johtopäätöksissä keskitytään ymmärtämään asioiden merkityksiä. (Tuomi & Sarajärvi, 2018, s. 94.)

## 3.4 Tutkimusprosessi

Tuomen ja Sarajärven (2018) mukaan yleisimmät menetelmät aineiston keräämiseksi ovat erilaiset haastattelut, kyselyt ja havainnointi sekä erilaisista dokumenteista kootut tiedot ja näiden kaikkien aineistojen analyysiin voidaan käyttää sisällönanalyysiä (Tuomi & Sarajärvi, 2018, s. 62). Tässä tutkimuksessa tutkimusaineisto kerätään tämän määritelmän mukaan erilaisista dokumenteista, jotka ovat tutkimusongelman määrittelyn perusteella tiedustelulait ja näihin liittyvät lakien esitöiden keskeiset asiakirjat. Laadullisessa tutkimuksessa ei pyritä tilastolliseen yleistykseen, vaan kuvaamaan tutkittavaa ilmiötä tai ymmärtämään tiettyä toimintaa (Tuomi & Sarajärvi, 2018, s. 73).

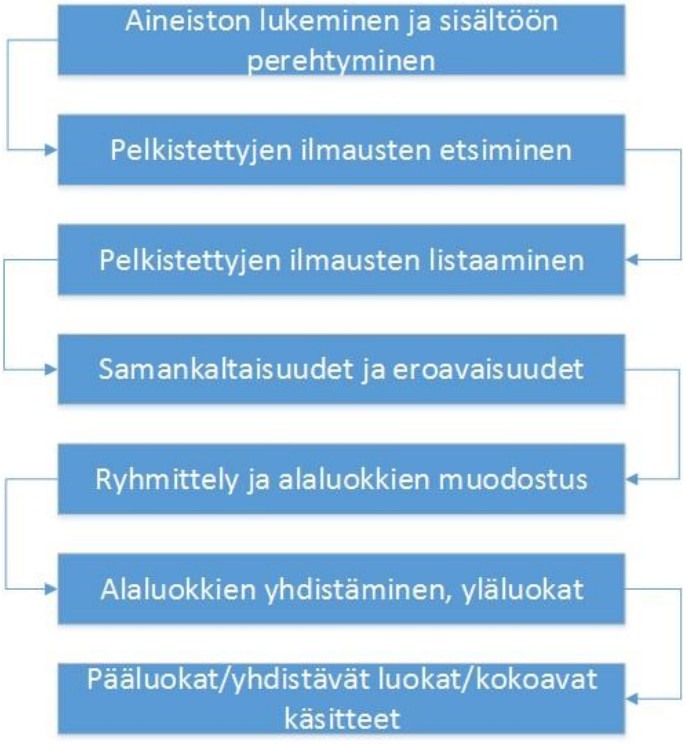
Tuomen ja Sarajärven (2018) mukaan sisällönanalyysin tarkoituksena on järjestää tutkimusaineisto tiiviiseen ja selkeään muotoon siten, että aineiston sisältämä informaatio säilyy. He myös korostavat sekä Burnsin ja Groven (1997) että Straussin ja Corbinin (1998) näkemystä siitä, että aineiston analyysin

tavoitteena on lisätä informaatioarvoa luomalla aineistosta selkeää ja yhtenäistä informaatiota tutkittavasta ilmiöstä. Aineiston selkeyttämisellä tavoitellaan sitä, että aineistosta voidaan tehdä luotettavia johtopäätöksiä. Analyysi perustuu loogiseen päättelyyn, jossa aineistoa aluksi pilkotaan ja lopuksi kootaan uudelleen selkeäksi kokonaisuudeksi. Analyysiä ei myöskään voida erottaa omaksi tutkimuksen vaiheeksi, vaan sitä tehdään kauttaaltaan tutkimusprosessin aikana. (Tuomi & Sarajärvi, 2018, s. 91.)

Tutkimusprosessin vaiheet perustuvat Tuomen ja Sarajärven (2018) kuvaamaan sisällönanalyysiin (ks. kuvio 4). Tutkimus aloitetaan määrittelemällä ajatuskokonaisuudet, jotka toimivat aineiston systemaattisen tarkastelun lähtökohtina. Ajatuskokonaisuudet ovat ennakko-oletuksia sille, mitä aineistosta halutaan etsiä. Ajatuskokonaisuudet ohjaavat tutkimusaineiston analyysiä, joten loogisesti ajatuskokonaisuuksiksi määritellään tutkimuksen alussa esitetyt tutkimuskysymykset:

1. Mitä sotilas- ja siviilitiedustelulaissa sanotaan avointen lähteiden tiedustelusta?

2. Mitä laeista käy ilmi liittyen avointen lähteiden tiedustelun tukevaan rooliin tiedustelutoiminnassa?




KUVIO 4 Mallikuva aineistolähtöisen sisällönanalyysin etenemisestä (mukaillen Tuomi & Sarajärvi, 2018, s. 91-92)

Käsiteltävään aineistoon perehdyttiin manuaalisesti, systemaattisesti perehtymällä. Luku- ja perehtymisprosessin aikana aineistosta taltioitiin tutkimuksen

kannalta olennaisia alkuperäisilmauksia erilliseen taulukkoon. Aineistosta nousseiden ilmauksien taulukointiin käytettiin Excel -taulukkolaskentaohjelmaa. Ilmauksiin sisällytettiin myös lähdeviittaukset asiakirjoihin, jotta yhteys alkuperäiseen aineistoon säilyi. Ilmauksien yläpuolelle merkittiin alkuperäinen asiakirja, josta tieto taltioitiin ja loppuun merkittiin alkuperäisen asiakirjan sivunumero. Joissain tapauksissa asiakirjoista ei ollut mahdollista kopioida haluttua kohtaa Excel -taulukkoon, jolloin ilmauksen tallennus toteutettiin kuvankaappauksena asiakirjasta ja liitettiin osaksi taulukkoa. Aineistosta taltioitujen ilmauksien arvioiminen sivumäärällisesti tai muutenkaan pituudellisesti oli haastavaa, sillä ilmaukset olivat pituudeltaan hyvin eri mittaisia ja ilmaukset sijoitettiin Excel -taulukkoon, mutta taulukossa oli aineiston läpikäynnin jälkeen yhteensä 618 riviä. Käsiteltävä aineisto sisälsi kokonaisuudessaan 489 asiakirjaa, mutta osa asiakirjoista oli päällekkäisiä siviili- ja sotilastiedustelulakien esitöiden välillä. Tämä johtui lakien läheisestä kytkennästä toisiinsa. Päällekkäisyyksistä huolimatta selkeyden vuoksi kaikki asiakirjat käytiin siitä huolimatta läpi.

Aineistoon perehtymisen jälkeen taltioituja alkuperäisilmauksia ryhdyttiin pelkistämään muodostamalla pelkistettyjä ilmauksia, jotka listattiin taulukkoon alkuperäisilmausten kanssa. Aineiston pelkistämisen tavoitteena oli pienentää aineiston kokoa, poistamalla ilmauksista epäolennaisia sanoja tai lauseita. Pelkistämistä ei kuitenkaan haluttu ylikorostaa, jotta aineiston informatiivinen arvo säilyisi seuraaviin analyysivaiheisiin. Myös pelkistämisen aikana yhteys alkuperäiseen lähteeseen säilytettiin.

Seuraavaksi tutkimusprosessissa siirryttiin ryhmittelyyn ja alaluokkien muodostukseen. Tämän tutkimusprosessin vaiheen tarkoituksena oli luokitella samankaltaisia ilmauksia aineistosta yhteen. Aluksi kaikille ilmauksille määritettiin ilmausta kuvaava luokka tai luokat, jonka jälkeen samankaltaisesti luokitellut ilmaukset ryhmiteltiin yhteen. Myös tässä tutkimuksen vaiheessa yhteys alkuperäiseen asiakirjaan säilytettiin. Jos samasta asiakirjasta oli useampia ilmauksia, merkittiin asiakirjan tiedot vain ensimmäisen ilmauksen yläpuolelle ja ilmauksien loppuun niiden sivunumerot alkuperäisestä aineistosta. Ilmauksia liikuteltiin Excel -taulukossa kopioimalla ja liittämällä.

Ryhmittelyn ja alaluokkien muodostuksen jälkeen tutkimusprosessissa edettiin seuraaviin luokitteluvaiheisiin. Luokittelua jatkettiin alaluokkien muodostuksen jälkeen ylätason luokitteluun. Alaluokista muodostui yläluokkia ja yläluokista muodostui yhteensä viisi pääluokkaa. Luokittelusta muodostettiin kaavio, joka kuvasi aineiston käsitteellisenä järjestelmänä. Kaavio on esitetty tarkemmin seuraavassa luvussa tutkimustulosten esittelyn yhteydessä. Aineiston analyysin tavoitteena oli sisällönanalyysin määrittelyn mukaisesti lisätä informaatioarvoa siten, että aineistosta luodaan selkeä ja informatiivinen kokonaisuus. Tällä aineiston luokittelulla ja järjestelyllä luotiin pohja sille, että järjestellystä aineistosta oli mahdollista esittää luotettavia johtopäätöksiä. Sisällönanalyysi tässä tutkimuksessa perustui sen määrittelyn mukaisesti loogiseen päättelyyn, jossa aineisto aluksi käytiin järjestelmällisesti läpi ja pilkottiin pieniin ilmauksiin. Tämän jälkeen aineisto koottiin jälleen yhteen luokittelemalla pilkotut ilmaukset samojen luokkien alle ja näin samankaltaiset asiat aineistosta ryhmittyivät

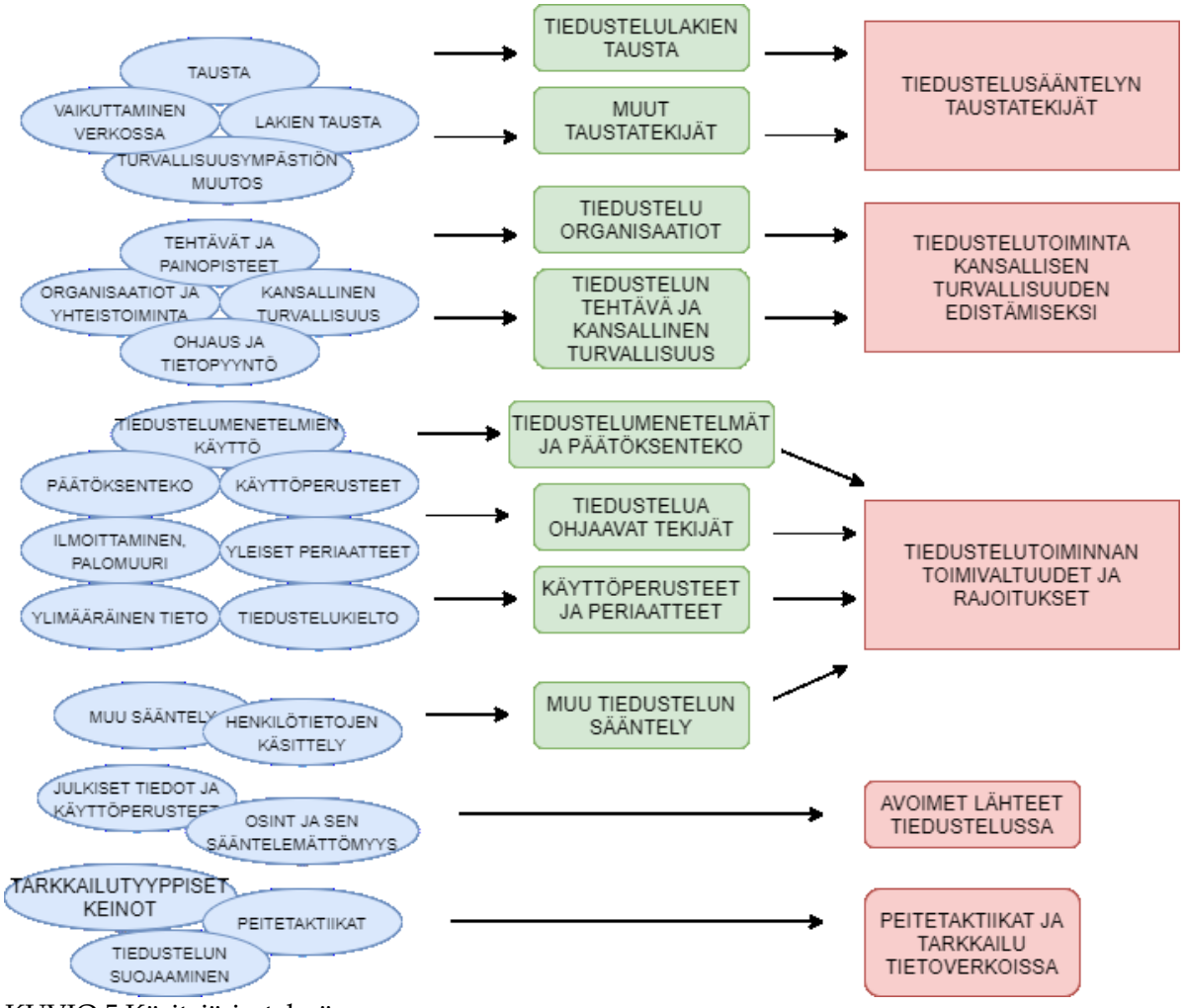
tiettyjen asiakokonaisuuksien alle selkeäksi kokonaisuudeksi. Näin ollen analyysiä ei pidetty tässä tutkimuksessa omana tutkimusvaiheenaan, vaan analyysiä tehtiin kauttaaltaan koko tutkimuksen ajan, jotta samankaltaiset asiakokonaisuudet kyettiin ryhmittelemään mielekkäästi yhteen. Lopuksi luokittelujen jälkeen muodostettiin yhdistävä luokka, joka vastasi tutkimuksen tutkimusongelmaan johtopäätösten muodossa luvussa 5. Yhdistävää luokkaa pidettiin tässä tutkimuksessa sisällönanalyysin määrittelyn mukaisesti kokoavana luokkana, johon sisältyy pääluokkien olennaisimmat huomiot suhteessa tutkimusongelmaan.

Sisällönanalyysin avulla kyettiin järjestelemään tiedustelulainsäädännön taustatekijät samaan luokkaan, jolloin esimerkiksi tutkimalla taustatekijöitä, voidaan tunnistaa avointen lähteiden tiedustelun käyttökohteita. Vastaavasti tutkimalla toimivaltuussääntelyä tiedustelutoiminnassa laajemmin, voidaan perustella avointen lähteiden tiedustelun sääntelemättömyyttä ja suhdetta toimivaltuussääntelyyn.

# 4 TUTKIMUSTULOKSET

Tässä luvussa käsitellään tutkimusprosessin tuloksena tuotettua analyysia. Analyysin tuloksena syntyy asiakokonaisuuksien käsitteellinen järjestelmä, joka perustuu aineiston ilmauksiin, joita taltioitiin alkuperäisistä asiakirjoista Excel -taulukkoon yhteensä 618 riviä.

Alla olevassa kuviossa (kuvio 5) on esitetty käsitejärjestelmä, joka aineiston luokittelun tuloksena syntyi. Käsitejärjestelmän perusteella myös muodostetaan tämän luvun rakenne. Kuvioon merkittiin sinisellä värityksellä alaluokat, vihreällä yläluokat ja punaisella pääluokat. Muusta luokittelusta poiketen, pääluokat ”avoimet lähteet tiedustelussa” sekä ”peitetaktiikat ja tarkkailu tietoverkoissa” nousivat voimakkaasti aineistosta, koska niistä löydettiin selkein yhteys tutkimusongelmaan. Näin ollen kuviossa esitetty suoraviivaistettu luokittelu katsottiin loogiseksi vaihtoehdoksi näiden luokkien osalta.




KUVIO 5 Käsitejärjestelmä

## 4.1 Tiedustelusääntelyn taustatekijät

Tässä alaluvussa käsitellään tiedustelulakivalmistelun taustalla vaikuttaneita tekijöitä. Luokittelun perusteella taustatekijät voidaan karkeasti jakaa kahteen luokkaan, lainsäädännölliset taustatekijät ja muut taustatekijät, kuten turvallisuusympäristön muutokset ja erilaiset vaikuttamiskeinot.

### 4.1.1 Lainsäädännöllinen tausta

Tiedustelulainsäädännön valmistelussa käsiteltiin useita hallituksen esityksiä, jotka liittyivät vahvasti toisiinsa. Käsiteltävät esitykset olivat sotilastiedustelua koskeva hallituksen esitys (HE 203/2017 vp), siviilitiedustelua koskeva hallituksen esitys (HE 202/2017 vp), Suomen perustuslain 10 §:n muuttamista koskeva hallituksen esitys (HE 198/2017 vp) sekä hallituksen esitys laiksi tiedustelutoiminnan valvonnasta ja laiksi valtion virkamieslain 7 §:n muuttamisesta (HE 199/2017 vp) (Mykkänen, 2018, s. 2). Tätä hallituksen esitysten kokonaisuutta on kutsuttu esitöissä myös tiedustelulakipaketiksi. Eräsen (2018) mukaan hallituksen esitykset pohjautuvat niin kutsutun tiedonhankintalakityöryhmän työhön, josta käytettiin nimeä ”Suomalaisen tiedustelulainsäädännön suuntaviivoja, Puolustusministeriö 2015”. Työryhmän työn jälkeen työtä jatkettiin jakaantuneesti eri esityksiin, jotka edellä on kuvattu (Eränen, 2018, s. 1). Mutasen (2018) mukaan tiedustelulainsäädännön valmistelun kokonaisuuteen kuului lisäksi vielä tiedustelutoiminnan parlamentaarisen valvonnan järjestämiseksi eduskunnassa valmisteltu puhemiesneuvoston ehdotus eduskunnan työjärjestyksen muuttamisesta (PNE 1/2018 vp). Mainituissa lainsäädäntöhankkeissa on lisäksi tehty tiivistä yhteistyötä eri ministeriöiden kesken. Ministeriöt olivat sisäministeriö, puolustusministeriö ja oikeusministeriö (Mutanen, 2018b, s. 1). Päätös lakihankkeiden jaosta tehtiin 20.8.2015 tiedustelulainsäädäntöhanketta käsittelevässä hallituksen strategiakokouksessa (HE 203/2017 vp, s. 6).

Nordströmin (2018) mukaan sisäministeriön vastuulla oli siviilitiedustelulaki, jossa luontevaa oli hyödyntää jo olemassa olevaa poliisilakia ja lisäksi laatia uusi erillinen laki tietoliikennetiedustelusta. Sotilastiedustelun osalta taas vastuussa oli puolustusministeriö, joka lähti puhtaalta pöydältä rakentamaan täysin uutta lainsäädäntöä sotilastiedustelusta (Nordström, 2018d, s. 1). Nordström (2018) myös toteaa, että erityisesti hallituksen esitykset siviili- ja sotilastiedustelulainsäädännöksi (HE 202/2017 vp ja HE 203/2017 vp) on valmistelu tiiviissä yhteistyössä sisä- ja puolustusministeriön kesken ja ehdotukset vastaavat keskeisiltä osilta toisiaan, pois lukien säädösteknisistä ratkaisuista johtuvat eroavaisuudet sotilastiedustelun kohteista ja erityispiirteistä (Nordström, 2018b, s. 1). Oli myös tunnistettu, että ehdotuksissa tulee olemaan hyvin samansisältöistä sääntelyä ja ehdotusten yhteensovittamisessa pyrittiin samojen ilmaisujen käyttöön, mutta tulevassa tiedustelutoiminnassa myös tunnistettiin paljon eroavaisuuksia esimerkiksi tiedustelun kohteissa, jolloin oli luontevaa laatia kaksi erillistä ehdotusta (Nordström, 2018d, s. 1; Meriniemi, 2018g, s.1).

Hallituksen esityksessä HE 202/2017 vp todetaan, että molemmat tiedustelusääntelyä koskevat ehdotukset liittyvät toisiinsa erityisesti tiedustelumenetelmien ja niihin liittyvien sääntelyjen osalta. Tiedustelumenetelmien sääntelyyn liittyen oikeusministeriössä valmisteltiin esitystä perustuslain muuttamisesta. Muutosehdotus kohdistui luottamuksellisen viestin rajoittamiseen tiedon hankkimiseksi sotilaallisesta toiminnasta ja muusta kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Tällä muutoksella tavoiteltiin sitä, että välttämättömistä luottamuksellisen viestin salaisuuden suojaan puuttuvista tiedustelumenetelmistä olisi edes mahdollista laissa säätää. (HE 202/2017 vp, s. 162.)

### 4.1.2 Turvallisuusympäristön muutos

Suomen turvallisuusympäristössä on kokonaisuudessaan tapahtunut merkittäviä muutoksia, joka asettaa suurempia vaatimuksia viranomaisille. Aiemmin tiedustelulainsäädäntöä ei Suomessa ole ollut. Turvallisuusympäristön merkittäviä muutossuuntia on esitetty lakien valmisteluissa useilta osa-alueilta.

Tiedustelusääntelyn valmisteluissa todetaan, että aiemmat viranomaisten toimivaltuudet perustuivat rikostorjuntaan, joka ei mahdollistanut tiedustelullisen toiminnan toteuttamista. Turvallisuusympäristön muutokset vaativat mukautumista myös kansallisen turvallisuuden turvaavilta tahoilta, jotta uhkista saadaan tietoa riittävän varhaisessa vaiheessa. Muuttunut turvallisuusympäristö ja siihen liittyvät epävarmuustekijät korostavat objektiivisen, varmennetun ja analysoidun tiedon tarvetta Suomeen kohdistuvista uhkista sekä päätöksenteon tueksi. (HE 202/2017 vp, s. 68.) Tiilikainen (2018) pitää Suomen tiedustelutoimintaan liittyvän suorituskyvyn laajentamista ja vahvistamista perusteltuna, sillä käsillä on useita muutoksia, jotka lisäävät toimintaympäristöjen arvaamattomuutta ja ennakoimattomuutta. Tiilikainen myös toteaa, että konfliktipotentiaali lisääntyy Suomen lähialueilla suurvaltapoliittisten jännitteiden takia sekä ulkoisen- ja sisäisen turvallisuuden välinen raja on hämärtynyt. (Tiilikainen, 2018, s. 4.)

Kansainvälistyminen ja tekninen kehitys ovat sivutuotteena aiheuttaneet muutoksia myös Suomen turvallisuusympäristössä. Vakavimmat kansalliseen turvallisuuteen kohdistuvat uhat ovat HE 203/2017 vp:n mukaan lähes poikkeuksetta kansainvälistä alkuperää. Globaali tekninen kehitys on myös mahdollistanut sen, että pienetkin valiolliset ja ei-valtiolliset toimijat kykenevät toimimaan tehokkaasti. Lisäksi kansallista turvallisuutta uhkaavat teot voivat toteutua nopeammalla aikataululla. Turvallisuuden ylläpitäminen nykymaailmassa vaatii ponnisteluja kaikilla politiikan osa-alueilla sekä kansallisesti, että kansainvälisesti. Esimerkiksi v. 2009 on tullut voimaan Lissabonin sopimus (SopS 66 ja 67/2009), joka on vahvistanut Euroopan unionin roolia turvallisuusuhkien torjunnassa. Lisäksi mm. Euroopan unionin yhteisvastuulauseke ja keskinäisen avunannon lauseke ovat edistäneet EU:n luonnetta yhtenäisenä turvallisuusyhteisönä. (HE 203/2017 vp, s. 5.)

Viimeisimmät merkittävimmät muutokset turvallisuusympäristössä ovat sisäisen turvallisuuden selonteon mukaan kyberuhat, laajamittainen laiton maahantulo, kansainvälinen terrorismi sekä Venäjän ja lännen suhteiden

huononeminen. Valtiollisessa vaikuttamisessa käytettävät hybridi- ja informaatiovaikuttamisen keinot ovat myös lisääntyneet, joihin vastaamiseksi tiedusteluviranomaisilla tulee olla riittävät voimavarat. Keskeisiä sisäiseen turvallisuuteen vaikuttavia tekijöitä ovat myös esimerkiksi digitalisaatio, kyberturvallisuus, huoltovarmuus ja perusinfrastruktuuri sekä näiden tekijöiden voimistunut keskinäisriippuvuus. Myös ulkomaisten tiedustelupalveluiden toiminta on Suomessa merkittävässä osassa ja sen kuvataan olevan samalla tasolla kuin kylmän sodan aikana. Muuttunut tilanne korostaa valtiollisen päätöksenteon ja ulkorajojen koskemattomuuden turvaamisen merkitystä. (HE 202/2017 vp, s. 9.)

Ulkomaisten tiedustelupalveluiden toimintaa Suomessa on kuvattu aktiiviseksi ja sen keskeiset mielenkiinnon kohteet ovat esimerkiksi Nato-jäsenyys, energiapoliittiset päätökset, energiahuoltovarmuus ja kyberturvallisuusrakenteet. Suojelupoliisilla on tiedossa konkreettisia tapauksia, joissa vieraat valtiot pyrkivät saamaan suomesta salaisia tietoja. Suomessa toteutettavan laittoman tiedustelutoiminnan torjuminen on myös monimutkaistunut. (Laitinen, 2018a, s. 3.)

Pelttari (2018) toteaa, että suurvaltojen käytös ja niiden väliset suhteet ovat aiempaa arvaamattomampia, joka asettaa geopoliittisesti arkaluontoisessa asemassa olevat maat vaaraan. Esimerkiksi kansainvälisten poliittisten jännitteiden painopiste on siirtynyt pohjoiseen Itämeren alueelle, jolla on heikentävä vaikutus Suomen lähialueiden turvallisuustilanteelle. (Pelttari, 2018a, s. 1.) Alueella on tapahtunut sotilasstrategista kehitystä ja sotilaallinen toiminta on vilkastunut alueella. Turvallisuusympäristön isona tekijänä nähdään edelleen Suomen itänaapuri Venäjä, joka on osoittanut kykynsä nopeisiin strategisiin päätöksiin. Lisäksi Venäjä on osoittanut kykynsä käyttää koordinoidusti sotilaallista voimaa ja laajasti muita keinoja tavoitteidensa saavuttamiseksi. Sodan kuva on selvästi monipuolistunut, sillä ns. sotatilanteessa käytettäisiin erittäin todennäköisesti sekä sotilaallisia, että ei-sotilaallisia keinoja yhdessä. Turvallisuusympäristön muutoksen ohella yhteiskunnan haavoittuvuus on lisääntynyt ja kybertoimintaympäristön merkitys kasvanut. Yhteiskunnan elintärkeät toiminnot ovat nykyään alttiita kybervaikuttamiselle, sillä digitalisaatio ja teknisten järjestelmien riippuvuussuhteet ovat jatkuvasti kasvaneet. Kyber- ja informaatiovaikuttamista on jo kohdistettu Suomeen mm. kansalaisia, poliittista päätöksentekojärjestelmää, kriittistä infrastruktuuria ja teollisuuslaitoksia vastaan. Yhteiskuntaa voidaan nykyään kuvata ympäristöksi, jossa perinteiset palvelut ja toiminnot ovat tietoteknisesti ohjattavissa tai ne toimivat kokonaan tietoverkoissa (HE 203/2017 vp, s. 9). Uusien tietoverkkojen vaikuttamismahdollisuuksien lisäksi ei tule unohtaa muita vakavia uhkia, joita ovat myös nk. CBRN-uhkat, eli kemialliset, biologiset, radiologiset ja ydinaseuhkat. (HE 203/2017 vp, s. 7.)

Yhteiskuntajärjestystä voi uhata myös tiettyä kansanryhmää vastaan osoitetut valeuutiset ja niiden levittäminen. Esimerkiksi eräässä tapauksessa Facebookissa levitettiin vihamielistä materiaalia, jolla on tietojen mukaan voinut olla ratkaiseva vaikutus Myanmarin rohingya-vähemmistön vainoamiseen. Tästä tapauksesta on raportoinut brittiläinen The Guardian. (Mielonen, 2018, s. 3.)

Laitisen (2018) mukaan sisäisen turvallisuuden strategia on hyväksytty vuonna 2017, joka pohjautui vuoden 2016 sisäisen turvallisuuden selontekoon ja näiden mukaan uudet haasteet vaativat viranomaisilta riittävää suorituskykyä. Laitisen mukaan globalisoitumiskehitys aiheuttaa sen, että yksittäisen valtion turvallisuuskysymys voi vaikuttaa myös kansainvälisesti. Vakavimmat kansallista turvallisuutta uhkaavat tekijät ovat myös nykyään usein voimakkaasti kytkeytyneet ulkopuolisiin tapahtumiin. Ulkopuoliset tapahtumat voivat myös olla vaikeasti hahmotettavia. Kansalliseen turvallisuuteen kohdistuvat uhkat voivat toteutuessaan aiheuttaa mittavaa vahinkoa. Esimerkiksi Ranskassa tapahtuneiden terrori-iskujen aiheuttama vahinko oli arviolta 750 miljoonaa euroa pelkästään turismin vähentymisen seurauksena. Ennen tiedustelulainsäädännön voimaantuloa Suomen mahdollisuudet reagoida kansallisen turvallisuuden uhkiin olivat epäsuhdassa mahdollisten toteutuneiden vahinkojen kanssa. Turvallisuusympäristön muutoksiin tulee kyetä vastaamaan asianmukaisella suorituskyvyllä, jotta valtion johdolle ja turvallisuudesta vastaaville viranomaisille on tarjolla riittävä tilannekuva mahdollisista uhkista. (Laitinen, 2018a, s. 2.)

Puistola (2018) on myös todennut, että terroritekoja valmistellaan piilossa, mutta tekijät voivat hankkia lähipiiriltään tai verkosta ohjeita, inspiraatiota ja hyväksyntää (Puistola, 2018, s. 4). Tämä korostaa entisestään tiedusteluviranomaisten riittävää asemaa ajantasaisen tiedon hankkimiseksi ja turvallisuutta uhkaavien tekojen ennalta estämiseksi. Turvallisuusympäristön muutoksessa korostuu erityisesti tietoverkkojen rooli.

### 4.1.3 Kyber- ja hybridivaikuttaminen

Kyberuhkat on tunnistettu mahdolliseksi uhkaksi jo vuonna 2010 yhteiskunnan turvallisuusstrategiassa, jossa todettiin, että tietojärjestelmiin tehtävän tunkeutumisen voidaan katsoa täyttävän tietyissä olosuhteissa jopa sotilaallisen voimankäytön tunnusmerkit. (HE 202/2017 vp, s. 154.) Myös Limnell (2018) toteaa, että teknologisesti kehittyneet valtiolliset toimijat kykenevät sotilaalliseen toimintaan sekä fyysisessä että digitaalisessa maailmassa ja yleisiä vaikuttamisen keinoja ovat tietojen ja videoiden manipulaatio, tietojärjestelmiin murtautumiset, luottamuksellisten tietojen vuotaminen ja erilaiset järjestelmien toimintahäiriöt. Tietoverkoissa toimii laajasti myös erilaisia aktivisteja ja haktivisteja, joiden motiivina on mielenosoitus. Haktivisteilla voi olla kykyä myös laajempaan vaikuttamiseen digitaalisessa maailmassa. Limnell korostaa, että laiton toiminta on yhtä laitonta sekä fyysisessä että digitaalisessa maailmassa. Esimerkiksi äärijärjestö ISIS on todistettavasti hyödyntänyt tietoverkkoja propagandan levittämiseen, rekrytoimiseen, rahaliikenteeseen ja viestintään. Muun muassa Yhdysvalloissa ja Iso-Britanniassa arvioidaan, että ISIS pyrkii tulevaisuudessa vaikuttamaan myös kyberhyökkäyksillä. (Limnell, 2018, s. 2-4.)

Myös Ylitalo (2018) toteaa, että yhteiskunnassa on käsillä mm. digitalisaation, sosiaalisen median ja tekoälyn jatkuva kehitys, joka toisaalta parantaa elämänlaatua ja toisaalta mahdollistaa vaikuttamisen ja sabotaasin erityisesti kyberympäristössä (Ylitalo, 2018, s. 2). Myös Tammikko (2018) toteaa, että

kyberulottuvuus ja sen merkitys on voimistunut. Erityisesti tällä hän tarkoittaa sitä, että organisoitua toimintaa voidaan koordinoida verkossa eikä fyysisiä suhteita välttämättä tarvita. (Tammikko, 2018, s. 2.)

Valtioihin on kohdistunut useita valtiollisten toimijoiden tai niihin liittyvien tahojen toteuttamia kyberoperaatioita, jotka ovat olleet hyvin organisoituja ja suunniteltuja. Esimerkiksi Ukrainan, Georgian ja Viron suljettuihin viranomaisverkkoihin on kohdistettu hyökkäyksiä. Suomenkin turvallisuusympäristön kannalta merkittävät valtiot panostavat merkittävästi offensiivisten kyberkyvykkyyksien rakentamiseen. Kybertoimintaympäristön hyökkäyksellisiä operaatioita voidaan käyttää muun ohella poliittisten, taloudellisten ja perinteisten sotilaallisten voimakeinojen tukena. Kyberuhkia kuvataan aiempaa vaarallisemmiksi koko yhteiskunnan kannalta. Olennaista on se, että nykyään toimijoihin lasketaan olennaisesti myös valtiollisen tason toimijat. Kybertoimintaympäristössä tehdään myös kybervakoilua, jossa tekniikkana käytetään monipuolisia verkkohyökkäystyökaluja. (HE 202/2017 vp, s. 11.)

Hybridioperaatiot ovat kokonaisuuksia, joissa kyberoperaatioiden rinnalla hyödynnetään muita painostuskeinoja. Valtiot voivat esimerkiksi kyberoperaatioidensa rinnalla painostaa poliittisesti, taloudellisesti ja sotilaallisesti sekä vaikuttaa sosiaalisessa mediassa. (HaVM 36/2018 vp, s. 19.) Euroopan hybridiuhkien torjunnan osaamiskeskuksen johtajan Matti Saarelaisen (2018) mukaan hybridiuhkien lisääntyminen on osa Euroopan turvallisuusympäristön muutosta. Hybridivaikuttaminen on hyvin suunnitelmallista toimintaa, jota suorittaa valtiollinen tai ei-valtiollinen toimija. Samanaikaisesti voidaan hyödyntää useita vaikuttamisen keinoja kohteen heikkouksien hyödyntämiseksi ja omien tavoitteiden saavuttamiseksi. Painostuskeinoja voidaan hyödyntää laajasti, joita ovat esimerkiksi taloudelliset, sotilaalliset ja teknologiaan perustuvat keinot ja informaatiooperaatiot sekä sosiaalisen median hyödyntäminen. Hybriditaktiikoita käytetään laajasti osana voimapolitiikkaa eikä niinkään vain osana sotilaallista konfliktia. (Saarelainen, 2018, s. 1.)

Hybridivaikuttamista suorittavat tahot voidaan jakaa valtiollisiin ja ei-valtiollisiin toimijoihin. Hybridivaikuttamisen keinoja on paljon, joita ovat esimerkiksi sotilaalliset, taloudelliset, infrastruktuurilliset, kulttuurilliset, poliittiset ja informaatioon perustuvat keinot. Hybridivaikuttamisella tarkoitetaan suurvaltojen ja muiden poliittisten tai aseellisten ryhmittymien toimintaa, jolla tavoitellaan suurempaa vaikutusvaltaa, vastapuolen häirintää tai omien poliittisten ja sotilaallisten tavoitteiden saavuttamista. Uhkana ei kuitenkaan ole pelkästään valtiollisten toimijoiden toiminta, vaan todellisen uhkan muodostavat myös kyberrikolliset. Iso osa tiedustelulainsäädännön taustalla vaikuttavista muutostarpeista perustui juuri kyberuhkiin ja niiden havaitsemiseen. Ennen tiedustelulainsäädäntöä toimivaltuudet perustuivat henkilö- ja rikosperusteisiin, joilla ei ollut mahdollista kaikissa tapauksissa tunnistaa tai torjua valtiollisia hybridiuhkia. Suojelupoliisin hybridiuhkiin liittyvät mielenkiinnon kohteet painottuvat informaatiovaikuttamiseen, propagandaan ja kybertoimintaan. (Laitinen, 2018a, s. 5.)

Yhtenäiskulttuuri on murenemassa ja mediakentässä on meneillään sirpaloituminen, jotka luovat avoimeen yhteiskuntaan erilaista mediamaisemaa, jossa

valtion rooli keskeisenä auktoriteettina on vaarassa marginalisoitua. Informaatiosodan ja -vaikuttamisen sekä muun vihamielisen vaikuttamisen näkökulmasta tämä avaa mahdollisuuksia myös monille muille uusille vaikuttamisen keinoille. Yhteiskunnissa on manipuloitavia kohdeyleisöjä, koska ilmapiiri on polarisoitunut. Myös Jantunen (2018) toteaa, että yhteiskunnan polarisoituminen luo otollisen maaperän hybridivaikuttamiselle, jolloin esimerkiksi sosiaalisesta mediasta voidaan tunnistaa, maalittaa ja mobilisoida tyytymättömiä yleisöjä kustannustehokkaasti (Jantunen, 2018, s. 3). Tutkijat olettavat, että informaatiovaikuttaminen tulee entisestään yleistymään. (HaVM 36/2018 vp, s. 15.)

### 4.1.4 Informaatiovaikuttaminen

Informaatiovaikuttamista tai sen tavoitetta voi olla vaikea havaita. Vieraat valtiot voivat esimerkiksi toteuttaa toimenpiteensä siten, että kohdevaltio ei voi olla varma onko kyseessä vieraan valtion ohjattu tavoitteellinen operaatio vai ei. Esimerkiksi tällaisen operaation tavoitteena voisi olla kansalaismielipiteeseen vaikuttaminen järjestelmällisesti väärää tietoa levittämällä. (HE 203/2017 vp, s. 185.)

Esimerkiksi Yhdysvaltojen vaaleihin on pyritty informaatiovaikuttamaan kybervakoilulla saaduille tiedoilla. Kansalliselle turvallisuudelle merkittävä uhka on myös tietoverkoissa toteutettava sabotaasi ja tietojen vääristeleminen. (Laitinen, 2018a, s. 4.) Informaatiovaikuttamiseen sisältyy esimerkiksi disinformaation levittäminen, kulttuurillisen vaikutusvallan kasvattaminen, katkosten aiheuttaminen tietojärjestelmiin sekä muu hämmennyksen ja epävakauden aiheuttaminen. Konkreettisena esimerkkinä toiminnassa voidaan hyödyntää esimerkiksi ns. trolleja ja sosiaalista mediaa. Teknisen kehityksen ansiosta uusien vaikuttamiskeinojen kokoelma on hyvin laaja. Informaatiovaikuttaminen voidaan yhdistää myös kyberhyökkäyksiin siten, että hyökkäyksen tavoitteena on tietojen saaminen, joita voidaan hyödyntää informaatiovaikuttamisessa. Kyberhyökkäyksiä voidaan käyttää myös esimerkiksi vaalikampanjoiden aikana ehdokkaiden mustamaalaukseen. (Laitinen, 2018a, s. 5.)

Myös Aapio (2018) on todennut, että huomattavaa on informaatiovaikuttaminen, jota käytetään viranomaisten uskottavuuden murentamiseen ja väärien tietojen levittämiseen yhteiskunnallisesti tärkeistä aiheista. Esimerkiksi keinona voi olla esiintyminen poliisina virallisia tunnuskuvia käyttämällä. Tämän lisäksi voidaan pyrkiä vaientamaan kohde, joka voi olla yksittäinen virkamies ja tällä tavoitellaan laajempaa vaikutusta koko yhteiskuntajärjestelmän perusrakenteisiin ja toimivuuteen. Tietoverkkoja voidaan hyödyntää myös rikoksentekovälineiden ja kumppaneiden etsimiseen, rikosten suunnitteluun, yhteydenpitoon sekä vihapuheen ja ääriajattelun levittämiseen, joka saattaa vaikuttaa otollisten henkilöiden, esimerkiksi syrjäytyneiden - radikalisoitumiseen. (Aapio, 2018, s. 1-2.)

Informaatiovaikuttamista ei voida kutsua uudeksi ilmiöksi, mutta sen toteuttaminen ja vaikuttavuus ovat muuttuneet merkittävästi nykyisessä digitaalisessa toimintaympäristössä. Informaatiovaikuttamista voidaan yhdistää sekä

hybridi- että kybervaikuttamisen rinnalle. Vaikuttamiselle on tyypillistä, että päätöksentekoa pyritään ohjaamaan mm. disinformaation avulla tai levittämällä vaillinaista tietoa. Riippuen vaikuttamisen asteesta, voidaan puhua tässä yhteydessä jopa informaatiosodasta. Avoimessa yhteiskunnassa voi olla riittävää, että aiheutetaan hajaannusta yhteiskunnan sisälle, joka voi vaikeuttaa viranomaisten ja poliittisten johtajien työtä. Myös tilannekuvan jakaminen ja kokoaminen voi vaikeutua. Kun informaatiovaikuttamisella pyritään vaikuttamaan kansalliseen turvallisuuteen, tavoitteena voi olla vaikuttaa mm. päätöksentekijöihin ja päätöksentekoprosesseihin. Lisäksi olennaista on tavoitella tilannetta, jossa kohde saadaan tekemään itselleen haitallisia päätöksiä tai vaikuttajan kannalta myönteisiä päätöksiä. Vaikuttaminen voi olla suoran menettelyn lisäksi myös välillistä, jossa suuren yleisön avulla kohdistetaan vaikutus päätöksentekijöihin tai päätöksentekoprosesseihin. Sosiaalisessa mediassa voidaan yrittää esimerkiksi ennalta vaikuttaa vaalitulokseen Twitterin avulla. (HaVM 36/2018 vp, s. 14.)

Informaatiovaikuttamista voidaan kohdentaa niin sanotun trollaamisen avulla. Esimerkiksi toimittajat, jotka ovat uutisoineet informaatiovaikuttamisesta, ovat joutuneet itse informaatiohyökkäyksen kohteeksi. Trollaamisella voidaan vaikuttaa informaatiotoimijaan esimerkiksi kyseenalaistamalla tietojen oikeellisuutta tai hyökkäämällä suoraan henkilöpersoonaa tai uskottavuutta vastaan. Sananvapautta myös väärinkäytetään harjoittamalla kiusaamista Internetissä, uhkailemalla ja vainoamalla. (HaVM 36/2018 vp, s. 15.)

### 4.1.5 Sosiaalinen media ja viestintä

Tietoverkkoja hyödynnetään nykyään laajasti erilaisten vaikuttamisen keinojen toteuttamiseen. Yksi näkökulma on se, että tietoverkkoja hyödynnetään verkostoitumiseen ja viestintään, joilla mahdollistetaan vaikuttaminen. Tietoverkoissa viestitään suunnitelmista ja aikeista, jotka toteutetaan reaalimaailmassa. (HE 202/2017 vp, s. 11.)

Sosiaalisen median kehitys mahdollistaa monimuotoisemmat verkostoitumismahdollisuudet. Valtiolliset toimijat panostavat omiin moderneihin mediaorganisaatioihin, jotka levittävät propagandaa, käyttävät sosiaalista mediaa sekä ylläpitävät avoimia ja suljettuja keskustelukanavia. Verkostoituminen mahdollistaa helpon viestinnän tahojen välillä, toiminnan suunnittelun ja reaaliaikaisen koordinoinnin. (HE 203/2017 vp, s. 10.)

Sekä Suomessa että ulkomailla on lisääntynyt huolestuttava ilmiö, väenkokoontuminen, joka ilmenee esimerkiksi katupartioina ja näitä tapahtumia koordinoidaan tyypillisesti sosiaalisessa mediassa sekä yleisten televerkkojen ja salattujen pikaviestisovellusten avulla. Kokoontumiset vaarantavat yleistä turvallisuutta. Sosiaalisessa mediassa ja Internetissä muutenkin levitetään laajasti samoin ajattelevien ryhmittymien toimesta vihapuhetta, disinformaatiota etnisistä vähemmistöryhmistä, valtionjohdosta, viranomaisista ja muista yhteiskunnallisesti merkittävistä keskustelunaiheista, jotka voivat horjuttaa turvallisuutta ja turvallisuudentunnetta. Lisäksi Helsingin poliisilaitoksen mukaan yleistä on

rikos- ja muut vihjeet, joita annetaan jopa tahallaan vääränsisältöisinä. (Aapio, 2018, s. 5.)

Tammikon (2018) mukaan tutkimukset myös osoittavat, että ns. yksinäiset sudet saattavat kertoa radikaaleista suunnitelmistaan läheisilleen tai sosiaalisessa mediassa, joka viittaisi siihen, että tehokkaalla tiedustelulla voidaan mahdollisesti ehkäistä iskuja (Tammikko, 2018, s. 1).

Tammikon (2018) mukaan verkkoagitaattoreiden rooli korvaa perinteistä johtajuutta ja verkossa yleistyy polarisoitumista ja viholliskuvien syntyä edistävä propaganda. Varsinaista kyberterrorismia ei kuitenkaan voida toteuttaa ilman korkeaa osaamista, joka yleistyy myös aktivistien joukoissa. Lievempää väkivaltaa, kuten poliittista väkivaltaa toteutetaan aktiivisesti esimerkiksi SOME-kampanjoiden avulla pilaamalla yksittäisten poliittisten toimijoiden mainetta sekä uhkailemalla ja pelottelemalla. (Tammikko, 2018, s. 2.)

Merkittävä muutostrendi koskee myös Internet-ympäristön hajoamista, jossa Kiina ja Venäjä tavoittelevat oman Internet-ympäristönsä (ChinaNet, RuNet) luontia Yhdysvaltojen dominanssin vastapainoksi (Lehto, 2018, s. 6).

### 4.1.6 Huoltovarmuus ja kriittiset toiminnot

Fjäderin (2018) mukaan huoltovarmuuden keskeisenä tavoitteena on kyetä selviytymään vakavista poikkeusoloista kansallisten resurssien avulla. Suomi on kuitenkin riippuvainen kansantalouden linkittymisestä globaaleihin markkinoihin sekä erilaisten resurssien ja palveluiden tuonnista eli myös Suomi on osa globaalia arvoverkostoa. Tämä dynaaminen kokonaisuus koostuu hyödykkeiden kehittämisestä, tuotannosta ja vaihdannasta, jotka yhdistyvät raaka-aineiden, informaation, rahoituksen ja henkilöiden virroiksi. Suomi on sidottu osaksi globaalia virtaa, jossa häiriöt voivat kohdistua esimerkiksi materiaalien, logistiikan, informaation ja rahan liikkumiseen. Tässä dynaamisessa kokonaisuudessa esiintyvien häiriöiden vaikutus voi ulottua myös Suomeen. Pilvipalvelut yleistyvät jatkuvasti ja tämä lisää ylikansallistumista. Digitalisaation vuoksi mm. kriittiset tietojärjestelmät integroituvat syvästi kyberympäristön ylikansallisiin prosesseihin. Myös monet yhteiskunnan merkittävät toiminnot ja kriittiset infrastruktuurit, jotka niitä tukevat, ovat riippuvaisia Suomen ulkopuolisista resursseista, prosesseista ja rakenteista. (Fjäder, 2018, s.1.)

Fjäderin mukaan yhteiskunnan turvallisuusstrategian 2017 määrittelemät huoltovarmuuden, kriittisen infrastruktuurin ja talouden keskeisimmät uhat ovat vakavat häiriöt elintarvikehuollossa ja energiansaannissa, julkisen talouden rahoituksen saatavuuden ja kuljetuslogistiikan häiriöt, rahoitus- ja maksu järjestelmän sekä tietoliikenteen ja tietojärjestelmien vakavat häiriöt, kyberuhkat, suuronnettomuudet sekä luonnon ääri-ilmiöt ja ympäristöuhkat. Terrorismin ja yhteiskuntajärjestystä vaarantavan rikollisuuden katsotaan myös olevan keskeinen uhka. Energiasta, ICT-järjestelmistä, palveluista ja logistiikasta ovat riippuvaisia kaikki talouden kriittiset toiminnot, infrastruktuuri, ruoka- ja vesihuolto sekä sosiaali- ja terveyspalvelut. Maksupalveluiden keskeytyminen nähdään

myös kriittisenä, sillä sen häiriöt voivat keskeyttää kriittisten palveluiden saatavuuden. (Fjäder, 2018, s. 2-3.)

Eronen (2018) katsoo, että tiedustelulainsäädäntö edistää liiketoimintaympäristön vakautta ja turvallisuutta. Viranomaisten kyky paljastaa ja estää haitallista toimintaa, joka kohdistuu kotimaisiin yrityksiin ja niiden liiketoimintasalaisuuksiin, nähdään elinkeinoelämän ja kilpailukyvyn näkökulmasta myönteisenä. (Eronen, 2018, s. 2.)

## 4.2 Tiedustelutoiminta kansallisen turvallisuuden edistämiseksi

Aiemmassa luvussa esiteltiin niitä lainsäädännön taustalla vaikuttavia tekijöitä, joiden mukaan tiedustelulainsäädännön tarvetta perusteltiin. Turvallisuusympäristö on ollut vauhdikkaassa muutoksessa, jonka vuoksi tiedusteluviranomaisilla tulee olla riittävä kyky hankkia tietoja Suomeen kohdistuvista uhkista. Turvallisuusympäristön muutoksessa keskiössä ovat tietoverkot ja digitaalinen ympäristö. Tiedustelutoiminnan keskeisenä tavoitteena on hankkia tietoa kansalliseen turvallisuuteen kohdistuvista uhkista sekä pitää valtion ylin johto tietoisena Suomea koskevista kansallisista ja kansainvälisistä asioista.

Sotilastiedusteluviranomaisilla on käytössään myös tiedonhankintakeinoja, jotka eivät vaadi erityistä toimivaltuussääntelyä. Tällaisiin keinoihin lasketaan myös avointen lähteiden tiedustelu. Tässä tapauksessa on kyse tiedonhankinnasta, jonka ei katsota loukkaavan yksityisyyden suojaa. Näin ollen avointen lähteiden tiedustelusta ei perustuslain mukaan tarvitse lailla säätää. (HE 203/2017 vp, s. 218.) Avointen lähteiden tiedustelua käsitellään tarkemmin tulosten loppuosassa, mutta jo tässä vaiheessa on olennaista määritellä, mitä avointen lähteiden tiedustelulla tarkoitetaan suhteessa toimivaltuussääntelyyn. Seuraavissa luvuissa käsitellään tiedustelun toimivaltuuksia sekä tiedustelutoimintaa kokonaisuutena, jolloin on myös olennaista hahmottaa avointen lähteiden tiedustelun suhde toimivaltuussääntelyyn ja tiedustelumenetelmien käyttöperusteisiin.

### 4.2.1 Kansallinen turvallisuus

Tiedustelusääntelyssä viitataan usein kansallisen turvallisuuden käsitteeseen ja sen syvällinen ymmärtäminen on välttämätöntä esimerkiksi tiedustelumenetelmien käyttöedellytysten ymmärtämiseksi. Kansallisen turvallisuuden käsitettä on tarkasteltu sekä kansallisella että EU-tasolla.

Suojelupoliisi suorittaa tiedonhankintaa kansalliseen turvallisuuteen kohdistuvien uhkien estämiseksi ja paljastamiseksi (HE 202/2017 vp, s. 14). Samoin sotilastiedustelu suorittaa tiedonhankintaa kansallista turvallisuutta uhkaavasta toiminnasta, jota on mm. Suomen maanpuolustusta tai yhteiskunnan elintärkeitä toimintoja uhkaava toiminta (Ojanen, 2018, s. 10). Tärkein muutos toiminnan suorittamisen edellytyksiin tiedustelusääntelyn myötä on, että tiedusteluviranomaisten toiminnan edellytykset eivät enää ole rikos- ja henkilöperusteisia vaan

uhkaperusteisia. Henkilö- ja rikoslähtöisiä toimivaltuuksia sekä niiden muutosta on käsitelty tarkemmin luvussa 4.3.1.

Kansallista turvallisuutta vakavasti uhkaava toiminta voidaan määritellä siten, että uhkan konkretisoituessa kyseessä olisi rikos, mutta tekijä ei ole tiedossa tai siihen ei voida vielä kohdistaa yksilöityä rikosepäilyä. Määrittelyä voidaan jatkaa myös siten, että kyseessä oleva toiminta voi olla tiedossa, mutta sen tapahtumapaikka on toisen valtion alueella. Kyse voi olla myös toiminnasta, joka Suomen lain mukaan ei ole rikollista eikä voi sellaiseksi muodostua, mutta toiminnan tarkoituksena on esimerkiksi suomalaiseen ja ulkomaiseen kansalaismielipiteeseen vaikuttaminen levittämällä väärää tietoa Suomen politiikasta. (Laitinen, 2018a, s. 6; ks. myös Viljanen, 2018, s. 2.)

Kansallisen turvallisuuden käsitteellä tarkoitetaan myös sitä, että määritelty uhkaava toiminta kohdistuu yleisesti yhteiskuntaan ja ihmisyhteisöön eikä kehenkään yksilönä. Jos uhka kuitenkin kohdistuu esimerkiksi valtion johtoon, voi myös tällöin uhka aiheuttaa vakavaa uhkaa myös kansalliselle turvallisuudelle. (Laitinen 2018b, s. 11; HE 203/2017 vp, s. 206.)

Mutanen (2018) toteaa, että HE 198/2017 vp:n mukaan kansallista turvallisuutta vakavasti uhkaavalla toiminnalla tarkoitetaan kansanvaltaista yhteiskunta- ja valtiojärjestystä, yhteiskunnan perustoimintoja, suuren ihmismäärän terveyttä tai henkeä tai kansainvälistä turvallisuutta ja rauhaa uhkaavaa toimintaa. Lisäksi edellytetään, että toiminnalla on kytkentä Suomeen ja uhka kohdistuu Suomen kansalliseen turvallisuuteen siitä huolimatta, että toiminta voi tapahtua myös rajojen ulkopuolella. Kyse voi olla myös esim. Suomen turvallisuuden kantilta keskeisen valtion levottomuuksista, ulkomaisen tiedustelupalvelun toiminnasta, kansallista turvallisuutta vakavasti uhkaavasta terrorismiin liittyvästä toiminnasta tai väkivaltaisesta radikalisoitumisesta. (Mutanen, 2018c, s. 4.)

Yhteiskunnan tärkeimpiä suojattavia etuja on määritelty yhteiskunnan turvallisuusstrategiassa 2010. Etuihin kuuluu valtion itsemääräämisoikeus, joka tarkoittaa suvereenisuutta suhteessa ulkovaltoihin ja muista riippumatta käyttää omien rajojensa sisällä ylintä valtaa parhaalla katsomallaan tavalla. Myös valtion johtaminen, kv-toiminta, puolustuskyky, sisäinen turvallisuus, talouden ja infrastruktuurin toimivuus sekä väestön toimeentuloturva ja toimintakyky ovat keskeisiä suojattavia etuja. Näihin mainittuihin keskeisiin etuihin kohdistuva uhka määritellään kansallista turvallisuutta uhkaavaksi toiminnaksi. Keskeisiin suojattaviin etuihin kohdistuvien uhkien torjunnasta vastaavat viranomaiset määritellään kansallisen turvallisuuden viranomaisiksi. Uhkille yhteistä on se, että taustalla olevat valtiolliset ja ei-valtiolliset toimijat ja niiden tunnistaminen sekä erottaminen toisistaan on entistä haastavampaa, jolloin myös ennakoiminen muodostuu haasteellisemmaksi. (HE 203/2017 vp, s. 9.)

Kansallisen turvallisuuden uhkalla tarkoitetaan myös sitä, että kansallinen turvallisuus ei ole välittömässä vaarassa, jolloin tiedonhankintaa voidaan kohdistaa myös sellaiseen toimintaan, joka jatkuessaan voisi vaarantaa kansallista turvallisuutta. (HE 202/2017 vp, s. 115.)

Kansallisessa turvallisuudessa on kyse eräänlaisesta kollektiivisesta suojeluintressistä, jonka sisältö johdetaan kansalaisten perusoikeuksista. Kansallisen

turvallisuuden käsitettä kuvataan laajaksi ja osittain jäsentymättömäksi ja sen merkityssisältöä on täsmennetty vain vähän ylikansallisissa sopimuksissa. Kansallisen turvallisuuden käsite tulee saamaan ja saa tarkemman määrittelynsä uhkien kautta, muun muassa siksi, että merkityssisältö on muutoksessa globaalin ja yhteiskunnallisen muutoksen mukana. Globalisaation vuoksi sisäisen ja ulkoisen turvallisuuden välinen jaottelu on yhä häilyvämpää. Uhkien ja riskien aluetai paikkasidonnainen rajaaminen on myös vaikeampaa, koska taloudelliset, tekniset ja sosiaaliset järjestelmät ylittävät rajoja sekä ovat riippuvaisia toisistaan. Kansallista turvallisuutta uhkaava toiminta voidaan kuitenkin jakaa karkeasti kahteen erityyppiseen toimintaan, sotilaalliseen- ja siviilitoimintaan. Jaottelu ei kuitenkaan ole absoluuttinen, sillä kumpikin toimintamuoto voi muodostua vakavaksi uhkaksi kansalliselle turvallisuudelle. (HE 202/2017 vp, s. 164.)

### 4.2.2 Välttämättömyys- ja tuloksellisuusvaatimus

Mutasen (2018) mukaan perustuslakivaliokunta on lausunnossaan PeVM 4/2018 vp korostanut, että tiedonhankinta kansallista turvallisuutta vakavasti uhkaavasta toiminnasta voidaan säännöksen mukaan osoittaa vain sellaisen viranomaisen tehtäväksi, joka vastaa kansallisesta turvallisuudesta. Rajoitusedellytys myös linjaa, että tietoa voidaan hankkia vain sellaisesta toiminnasta, jonka luonne viittaa vakavasti kansallista turvallisuutta uhkaavan toiminnan muodostumiseen. Lisäksi lainsäädäntö linjaa tyhjentävästi toimivaltuuksien kohdentumisesta tällaiseen toimintaan ja sääntelyllä ei mahdollisteta kohdentamatonta kaikenkattavaa tietoliikenteen seurantaa. Perustuslakivaliokunta on myös samaisessa lausunnossaan korostanut välttämättömyysvaatimuksen toteutumista. Tällä vaatimuksella tarkoitetaan sitä, että luottamuksellisen viestin salaisuuteen voidaan puuttua vain niissä tapauksissa, missä tiedonhankinta ei yksinkertaisesti ole mahdollista vähemmän puuttuvin keinoin. Lisäksi luottamuksellisen viestin salaisuuteen saa puuttua vain mahdollisimman rajoitetusti ja kohdennetusti. Lisäksi rajoitusperusteeseen vetoaminen vaatii perustuslakivaliokunnan mukaan sen, että vetoajalla on esittää riittävät perusteet kyseessä olevan toiminnan muodostumisesta uhkaksi kansalliselle turvallisuudelle. Välttämättömyysvaatimuksen täyttymiseksi on kyettävä osoittamaan, että tiedon hankinnalla kussakin yksittäisessä tapauksessa ja siihen liittyvien yksilökohtaisten perusoikeuksien rajoitukset ovat tehokkaita ja toisaalta välttämättömiä keinoja hankkia kyseisessä tilanteessa tietoja toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Vaatimuksen täyttyminen ei perustuslakivaliokunnan mukaan toteudu pelkästään siten, että esitetään luottamuksellisista viesteistä kerätyn tiedon hankinnan yleistä kansallista turvallisuutta edistävää vaikutusta (Mutanen, 2018c, s. 4-5.)

Kaikille tiedustelumenetelmille on säädetty ns. perustelua edellyttävä tuloksellisuusvaatimus. Tiedustelumenetelmien käytön yleisenä edellytyksenä on, että menetelmällä voidaan perustellusti olettaa saatavan tietoja toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Mikä tahansa tiedustelun kohde ei itsessään muodosta säädöksen mukaan vakavaa uhkaa kansalliselle

turvallisuudelle, vaan jokaisen tiedustelumenetelmän kohdalla tulee osoittaa, kuinka kohdeluettelossa mainittu uhkaperuste ilmenee ja perustella se, kuinka kyseinen uhkaperuste muodostaa vakavan uhkan kansalliselle turvallisuudelle. (HE 202/2017 vp, s. 115.) Alla on esitetty yleinen tuloksellisuusvaatimus siten, kuin se on säädetty sekä siviili- että sotilastiedustelulainsäädännössä:

> 4 § (26.4.2019/581)
>
> Tiedustelumenetelmien käytön edellytykset
>
> Tiedustelumenetelmän käytön yleisenä edellytyksenä siviilitiedustelussa on, että sen käyttäminen on välttämätöntä tärkeiden tietojen saamiseksi sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. (Poliisilaki, 5 a luku, 2019.)
>
> 12 §
>
> Tiedustelumenetelmien käytön yleiset edellytykset
>
> Tiedustelumenetelmän käytön yleisenä edellytyksenä on, että tiedustelumenetelmän käyttö on välttämätöntä ja että sillä voidaan perustellusti olettaa saatavan tärkeää tietoa tiedustelutehtävän kannalta. Jos tiedustelumenetelmä kohdistetaan valtiolliseen toimijaan, tiedustelumenetelmän käytön yleisenä edellytyksenä on, että tietojen saaminen on tarpeen tiedustelutehtävän kannalta. (Laki sotilastiedustelusta, 2019.)

### 4.2.3 EU- ja kansainvälinen oikeus

Meriniemi (2018) toteaa, että kansallisen turvallisuuden käsitettä on käytetty lainsäädännössä jo aiemmin ja sitä käytetään myös EU:n oikeusjärjestyksessä ja kansainvälisissä ihmisoikeussopimuksissa ihmisoikeuksien rajoitusperusteena. Meriniemen (2018) ja Laitisen (2018b, s. 11) mukaan esimerkiksi tapauksessa Kennedy v. Yhdistynyt Kuningaskunta 18.5.2010 on käsitelty sitä, että Euroopan ihmisoikeussopimuksen tulkinnassa valtioille on katsottu olevan varsin laaja harkintamarginaali kansallisen turvallisuuden määrittelyyn. Mielivaltaista puuttumista yksilöiden luottamuksellisen viestin suojaan on kuitenkin pyritty rajoittamaan sillä, että Euroopan ihmisoikeustuomioistuin on asettanut vähimmäisvaatimuksia salaisia tiedonhankintakeinoja koskevalla lainsäädännölle. Tätä on Meriniemen mukaan käsitelty esimerkiksi tapauksessa Zakharov v. Venäjä 4.12.2015. (Meriniemi, 2018c, s. 21.)

Meriniemen (2018) mukaan esimerkiksi EU:n tuomioistuimen tuomiossa J.N. C-601/15 käsitellään sitä, että jäsenvaltiot eivät voi mielivaltaisesti ilman unionin toimielinten valvontaa määritellä, mitä yleisen ja kansallisen turvallisuuden ulottuvuuksilla tarkoitetaan. EU:n oikeuden soveltamisalalla yleisen ja kansallisen turvallisuuden käsitteitä tulee tulkita EU:n oikeuden ja EU:n tuomioistuimen oikeuskäytäntöjen valossa. Meriniemen mukaan kuitenkin poliisilain 5 a luvun 3 §:ssä kansallisen turvallisuuden alaan kuuluvat toiminnot on määritelty toimivaltuuksien käytön näkökulmasta tyhjentävästi. Hänen mukaansa myös

lakiehdotuksissa esitetty uhkaperusteinen määrittelytapa ja laissa määritellyt uhkat ovat sopusoinnussa EIT:n ratkaisukäytäntöjen kanssa. (Meriniemi, 2018c, s. 21.) Myös hallituksen esityksen mukaan 3 §:ssa mainitut kohteet eli perusteuhkat kuuluvat kansallisen turvallisuuden käsitteen alle, EIT:n esittämän käsitteen tulkinnan mukaisesti. Kohdeluettelo on tyhjentävä. (HE 202/2017 vp, s. 115.) Laitisen (2018) mukaan taas esimerkiksi tapauksissa Klass v. Saksa sekä Weber ja Saravia v. Saksa EIT:n ratkaisukäytäntö toteaa, että ainakin sotilaallinen maanpuolustus, terrorismin torjunta sekä laittoman tiedustelun torjunta lasketaan kansallisen turvallisuuden käsitteen alle (Laitinen, 2018b, s. 11).

Scheinin (2018) taas toteaa, että EU-oikeudessa kansallisen turvallisuuden kysymykset ovat viimekädessä jäsenvaltioiden toimivallan piirissä ja näin ollen EU:n tuomioistuimen vallan ja EU-perusoikeuskirjan soveltamisalan ulkopuolella. Hänen mukaansa tästä ei kuitenkaan seuraa sitä, että EU:n tuomioistuimen antamat linjaukset ovat merkityksettömiä sellaisen tiedustelutoiminnan kannalta, jota perustellaan kansallisen turvallisuuden käsitteellä. (Scheinin, 2018, s. 6.)

### 4.2.4 Yleiset periaatteet, perus- ja ihmisoikeudet

Poliisilain 1 luvussa on säädetty ns. poliisioikeudellisista periaatteista, perus- ja ihmisoikeuksien kunnioittamisesta, suhteellisuus-, vähimmän haitan- ja tarkoitussidonnaisuusperiaatteesta sekä mahdollisuudesta siirtää tehtävää tai luopua siitä. Yleisesti periaatteet koskevat kaikkea poliisivaltuuksien käyttöä sekä kaikkien poliisitehtävien hoitoa. Periaatteet ilmenevät myös välillisesti useissa poliisilain sisältämissä yksittäisten säännösten sanamuodoissa. Periaatteiden noudattaminen on korostetun tärkeää silloin, kun käytetään voimakeinoja, salaisia tiedonhankintakeinoja tai silloin, kun yleensäkin puututaan toimenpiteiden yhteydessä olennaisella tavalla kansalaisten oikeuspiiriin. (HE 202/2017 vp, s. 16; Meriniemi, 2018f, s. 4.) Yleisillä periaatteilla on korostunut merkitys silloin, kun käytetään tiedustelumenetelmiä (HE 202/2017 vp, s. 170).

Perus- ja ihmisoikeusnäkökulmaa korostetaan sellaisten toimivaltuuksien yhteydessä, joiden käyttö tapahtuu salaa niiden kohteelta, koska kyseiset toimivaltuudet puuttuvat usein perustavaa laatua olevien oikeuksien ydinalueelle (HE 202/2017 vp, s. 50). Sotilastiedustelun osalta yllä mainittujen periaatteiden lisäksi on mainittu myös syrjinnän kielto, mutta yleisesti sotilastiedustelussa tulee yhtä lailla kunnioittaa perus- ja ihmisoikeuksia sekä yleisiä periaatteita, ja ne vastaavat poliisilaissa esitettyjä vastineitaan (HE 203/2017 vp, s. 356; Nordström, 2018a, s. 5). Rönkä (2018) on lisäksi todennut, että Suomessa ja Euroopassa suojataan kansalaisten perusoikeuksia, kuten yksityisyyttä ja luottamuksellista viestintää, yhtä lailla myös tietoverkoissa (Rönkä, 2018, s. 1).

Suhteellisuusperiaatteella tarkoitetaan sitä, että toimenpiteiden oikeasuhtaisuutta tulee arvioida, ja haittojen, kuten yksityisyyden suojaan puuttumisen, on oltava järkevästi suhteutettua tavoiteltuun päämäärään nähden. Kyse on siitä, että tiedon saamiseksi käytettävän toimenpiteen tulee olla riittävän tehokas ja toimenpide ei saa olla ylimitoitettu kohteen näkökulmasta. Suhteellisuusperiaate ilmenee myös siten, että toimenpiteestä on oikeus luopua, mikäli toimenpiteen

loppuun saattaminen aiheuttaisi kohtuuttoman lopputuloksen päämäärän saavuttamiseksi. (HE 202/2017 vp, s. 170; Meriniemi, 2018f, s. 4.)

Vähimmän haitan periaatteella tarkoitetaan sitä, että toimenpiteiden on oltava välttämättömiä tehtävän suorittamiseksi, eli kenenkään oikeuksiin ei saa puuttua enempää kuin on välttämätöntä eikä kenellekään saa aiheuttaa suurempaa vahinkoa kuin on välttämätöntä. Oikeudet on määritelty perusoikeuksina perustuslaissa. Perusoikeuksiin puuttuminen on periaatteen mukaan minimoitava tiedustelumenetelmää käytettäessä ja periaate suojaa kaikkia, joihin toimenpiteellä on vaikutusta. Vähimmän haitan periaatteeseen liittyy tiivistetysti välttämättömyysedellytys ja optimointivelvollisuus, joka koskee tiedustelumenetelmien käyttöä. Näillä elementeillä ohjataan tiedustelumenetelmien valintaa ja kohdistamista. (HE 202/2017 vp, s. 170; Meriniemi, 2018f, s. 4; Viljanen, 2018, s. 2.)

Tarkoitussidonnaisuuden periaatteella tarkoitetaan sitä, että esimerkiksi poliisi saa käyttää toimivaltuuttaan vai säädettyyn tarkoitukseen, kuten esimerkiksi poliisin hallinosta annetussa laissa 10 §:ssä ja poliisilain 1 luvun 1 §:ssä todetaan, että suojelupoliisin toimivillan on perustuttava aina nimenomaiseen säädökseen. Silloin kun puututaan yksilön oikeuksiin tai velvollisuuksiin, on säännöksen oltava laissa. Periaate koskee myös yleisesti kaikkea toimintaa. (HE 202/2017 vp, s. 170; Meriniemi, 2018f, s. 4.)

Ojasen (2018) mukaan oikeudellisen ja erityisesti perus- ja ihmisoikeusjuridisen tarkastelun lähtökohtana täytyy korostaa sitä, että Suomen perustuslain lisäksi otetaan huomioon myös kansainväliset ihmisoikeusvelvoitteet, erityisesti Euroopan ihmisoikeussopimus ja sitä koskeva Euroopan ihmisoikeustuomioistuimen oikeuskäytäntö sekä EU:n oikeus, erityisesti EU:n perusoikeuskirja ja sitä koskeva EU-tuomioistuimen oikeuskäytäntö (Ojanen, 2018c, s. 1; ks. myös Ylitalo, 2018b, s. 4; Hyysalo, 2018, s. 3; Lavapuro, 2018, s. 3). Perustuslakivaliokunta on myös todennut, että oikeuskäytäntöä on suhteellisen runsaasti ja se kehittyy jatkuvasti (PuVM 9/2018 vp, s. 8).

Pohjolainen on asiantuntijalausunnossaan (2018) myös todennut, että perusoikeuksien yleisenä rajoitusedellytyksenä on vaatimus, jonka mukaan perusoikeusrajoitusten on oltava sopusoinnussa kansainvälisten ihmisoikeusvelvoitteiden kanssa. Erityinen merkitys tässä asiayhteydessä on Euroopan ihmisoikeussopimuksella, ihmisoikeustuomioistuimen oikeuskäytännön kannalta. Oikeuskäytännön mukaan luottamuksellisen viestin salaisuuteen puuttumisella täytyy olla aina painava yhteiskunnallinen tarve, tavoiteltavan hyväksytyn tavoitteen ja puuttumisen on oltava oikeassa suhteessa keskenään sekä puuttumiselle on löydyttävä riittävät ja hyväksyttävät perustelut. Tämän lisäksi rajoitusten tulee olla lainsäädännöllä sallittuja. (Pohjolainen, 2018, s. 8.)

Scheinin (2018) on pohtinut ihmisoikeuksia tiedustelutoiminnassa. Hänen mukaansa tietyn tarkkailuteknologian käyttö voi olla hyväksyttävää, jos sillä saavutetaan todellista hyötyä esimerkiksi kansalliselle turvallisuudelle ja teknologian aiheuttavat rajoitukset ihmisoikeuksien osalta ovat asteeltaan sellaisia, että saavutettavalla hyödyllä voidaan rajoituksia oikeuttaa. Hänen mukaansa myös ihmisoikeusrajoituksia koskeva suhteellisuusarviointi ei ole abstrakti arvojen

painojen vertailu, jossa vertaillaan esimerkiksi yksityisyyden suojaa suhteessa koko kansakunnan turvallisuuteen. Kyse on vertailusta ”yhteen yksilöön tai laajaankin joukkoon ihmisiä kohdistuvan ihmisoikeusrajoituksen ja rajoituksen perustana olevan hyväksyttävän tarkoituksen toteuttamiselle juuri tuon rajoituksen kautta saavutettavan hyödyn välillä”. Hänen mukaansa ei siis riitä, että rajoitus ihmisoikeuksiin palvelee kansallista turvallisuutta tai rajoituksen vain sanotaan palvelevan sitä. Lisäksi tulee osoittaa, että rajoitus on tehokas ja sillä voidaan saavuttaa jopa mitattava hyöty kansalliselle turvallisuudelle. Tällöin vertailu tehdään saavutettavan hyödyn ja ihmisoikeusrajoituksen välillä. Lisäksi on vielä huomioitava rajoituksen sisällöllinen kohdentuminen ihmisoikeuksia koskevassa sääntelyssä sekä rajoituksen aste. (Scheinin, 2018, s. 3.)

Scheinin (2018) on myös todennut, että esimerkiksi henkilötiedustelun avulla valitun henkilön Facebook-verkoston pohjalta suoritettu sähköisen viestinnän kohdennettu valvonta tuottaa paremman turvallisuushyödyn suhteessa kohdentamattomaan massavalvontaan sekä tuottaa hyväksyttävämmän rajoituksen ihmisoikeuksiin (Scheinin, 2018, s. 4). Scheinin viittaa kohdentamattomalla valvonnalla tietoliikennetiedusteluun, jota tässä tutkimuksessa ei käsitellä.

Hakosen (2018) mukaan turvallisuusviranomaisten säätelyn, joka koskee käytettäviä toimivaltuuksia, tulee olla tarkkarajaista ja täsmällistä. Toisaalta hän toteaa myös, että kansallista turvallisuutta vakavasti uhkaava toiminta on sellaista, johon on tarve puuttua varhaisessa vaiheessa. Uhkamäärittely jää näin ollen väistämättä osittain väljäksi. Tiedusteluviranomaisilla on myös tarve pitää tekniset ja taktiset tiedustelumenetelmät salassa, joka vaikuttaa myös toimivaltuussääntelyn avoimuusasteeseen. Hakonen myös korostaa, että tiedustelutoiminnassa ei ole varhaisessa vaiheessa perusoikeusnäkökulmasta kyse perusoikeus vs. toinen perusoikeus punninnasta, vaan laajemmasta asettelusta, jossa konkreettista perusoikeutta arvioidaan suhteessa abstrakteihin perusoikeusjärjestelmän olemassaolon edellytyksiin. (Hakonen, 2018, s. 1.)

Avointen lähteiden tiedustelusta ei perustuslain mukaan tarvitse laissa säätää, koska menetelmällä ei kajota yksilöiden perusoikeuksiin. Näin ollen myöskään tarkastelua perusoikeussuojan ja menetelmän tuottaman hyödyn välillä ei tarvitse tehdä. Avointen lähteiden tiedustelua voidaan myös käyttää kevyemmin, verrattuna sellaisiin tiedustelumenetelmiin, joilla puututaan lailla suojattuihin perusoikeuksiin.

### 4.2.5 Henkilötietojen käsittely

Siviilitiedustelussa käsitellään myös henkilötietoja, josta säädetään tiedustelulainsäädännön ohella uudistetussa poliisin henkilötietolaissa. Laissa on huomioitu myös EU:n tietosuoja-asetuksen ja tietosuojadirektiiviin aiheuttamat muutostarpeet. Laissa henkilötietojen käsittelystä poliisitoimessa säädetään kattavasti ja yksityiskohtaisesti siviilitiedustelua koskevasta henkilötietojen käsittelystä sekä henkilötietoja koskevasta käyttötarkoituksesta ja tietosisällöistä sekä muutamasta muusta seikasta liittyen henkilötietojen käsittelyyn. (HE 202/2017 vp, s. 271.)

Samantyyppisiä uudistuksia toteutettiin myös sotilastiedustelun osalta, sillä myös sotilastiedustelussa käsitellään henkilötietoja. Sääntely pohjautuu EU:n tietosuojaa koskevaan sääntelyyn. Puolustusvoimien osalta henkilötietojen käsittelystä sotilastiedustelussa säädetään henkilötietojen käsittelystä Puolustusvoimissa annetussa laissa sekä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa. Näistä jälkimmäistä sovelletaan tietysti myös siviilitiedustelun osalta. Näiden lakien muodostaman kokonaisuuden lisäksi ei sovelleta lainkaan EU:n tietosuoja-asetusta eikä yleistä tietosuojalakia. (HE 203/2017 vp, s. 350.)

## 4.3 Tiedustelutoiminnan toimivaltuudet ja rajoitukset

Aiemmassa luvussa kuvattiin syvällisesti, mitä kansallisen turvallisuuden käsitteellä ja kansallisen turvallisuuden suojaamisella tarkoitetaan. Tämän määrittelyn jälkeen voidaan käsitellä itse tiedustelumenetelmiä, joita kansallisen turvallisuuden suojaamiseen käytetään. Ensin tässä alaluvussa käsitellään tiedustelumenetelmiä ja niiden käyttöperusteita yleisesti ja sen jälkeen tarkastelu kohdistetaan avointen lähteiden tiedusteluun sekä muihin tietoverkkotaktiikoihin myöhemmissä luvuissa.

Tiedustelutoimivaltuuksia kuvataan kokonaisuudeksi, johon lasketaan useita eri tiedustelumenetelmiä toisiaan täydentäen. Pelkästään rikostorjunnallisilla toimivaltuuksilla ei kuitenkaan ole mahdollista saada kaikkea sellaista tarpeellista tietoa, jota tarvitaan kansallisen turvallisuuden tarpeeseen. (HE 202/2017 vp, s. 109.) Tämän vuoksi tärkeimpänä kehityskohteena tiedustelusääntelyn osalta oli irtaantua ns. rikosperusteisuudesta.

Tiedustelulainsäädännöllä ehdotettiin muutettavaksi suojelupoliisin toimivaltuuksia ja tehtäviä siten, että tehtäviin kuuluu myös tiedonhankinta kansallisen turvallisuuden suojaamiseksi. HE 202/2017 vp:ssä on myös todettu, että tietoa hankitaan edelleen avoimista lähteistä ja muilta viranomaisilta. (HE 202/2017 vp, s. 105.)

Aiemmin Puolustusvoimilla ei ole ollut erityisiä toimivaltuuksia tiedonhankintaan, vaan niiden on osin katsottu perustuvan Puolustusvoimien tehtäviin, jotka määriteltiin puolustusvoimista annetun lain 2 §:ssä. Rikostorjunnassa on kuitenkin voitu käyttää eräitä poliisille tiedonhankintaan säädettyjä toimivaltuuksia. (HE 203/2017 vp, s. 21-22.)

### 4.3.1 Henkilö- ja rikosperusteisuus vs. uhkaperusteisuus

Tiedustelulainsäädännön kannalta tehtiin olennainen lisäys perustuslain 10 §:ään, jossa 4 momentissa on koottu luottamuksellisen viestin salaisuutta koskevat rajoitusperusteet. Säännös mahdollistaa sen, että:

> Lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa,

> oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. (Suomen perustuslaki, 5.10.2018/817.)

Käytännössä tällä tarkoitetaan sitä, että sotilaalliseen toimintaan tai muuhun vakavasti kansallista turvallisuutta uhkaavaan toimintaan kohdistuvassa tiedonhankinnassa ja niiden rajoitusperusteissa irtauduttiin henkilö-, rikos- ja rikosepäilyperusteisuudesta (ks. myös Lavapuro, 2018, s.1). Rajoituslauseke mahdollistaa luottamuksellisen viestinnän rajoitukset tiedustelutoiminnassa. Perustuslakivaliokunta on lausunnossaan PeVM 4/2018 vp sivulla 7-8 todennut, että rajoitusperustetta on tarve tulkita suppeasti ja yleisten perusoikeuksien rajoitusedellytysten mukaisesti. Perustuslakivaliokunnan mukaan myös välttämättömyysedellytyksen vuoksi luottamuksellisen viestin salaisuuden suojaan puuttumisen tulee tapahtua mahdollisimman kohdennetusti ja rajatusti. (Mutanen, 2018c, s. 3.)

Tiedustelutoiminnan tyypillisenä tavoitteena on löytää henkilöt, jotka voivat aiheuttaa vakavaa uhkaa kansalliselle turvallisuudelle, eikä yksilöitä välttämättä ole mahdollista tunnistaa etukäteen. Tämän vuoksi tiedustelutoimivaltuuksien käyttöperusteet irrotettiin rikos- ja henkilökytkennästä. Lisäksi on pidetty tärkeänä, että yhteistyöverkostossa muiden maiden kanssa ollaan mukana verrokkimaita vastaavilla toimivaltuuksilla. Riittävillä toimivaltuuksilla voidaan myös osaltaan varmistaa sitä, että Suomen on mahdollista saada tietoa esimerkiksi kansalliseen toimintaan kohdistuvasta verkkovakoilusta, eikä tiedonsaanti ole kolmannen maan viranomaisten varassa. Verkkovakoilulla viitataan tässä asiayhteydessä vuoden 2013 tapahtumiin, jolloin kolmannelta maalta saatiin tieto Suomen ulkoministeriöön kohdistuneesta laajamittaisesta vakoilusta. (PuVL 16/2018 vp, s. 3.)

Suojelupoliisin tehtävä on sisäministeriön ohjauksen mukaisesti poliisin hallinnosta annetun lain 110/1992 10 §:n 1 momentin mukaan torjua hankkeita ja rikoksia, jotka voivat vaarantaa yhteiskunta- ja valtiojärjestystä taikka valtakunnan ulkoista tai sisäistä turvallisuutta sekä suorittaa tällaisten rikosten tutkinta. Suojelupoliisin aiemmat salaisten tiedonhankintakeinojen toimivaltuudet oli määritelty henkilö- ja rikoslähtöisesti, jolloin niitä voitiin kohdistaa vain sellaiseen henkilöön tai toimintaan, johon liittyy perustellusti oletus rikokseen syyllistymisestä tulevaisuudessa tai rikos on jo tapahtunut. Joissain tapauksissa oli mahdollista kohdistaa myös rikoksen valmisteluun. (Meriniemi, 2018a, s. 6).

Ennen tiedustelusääntelyn voimaantuloa Puolustusvoimienkin toimivaltuudet olivat rajoittuneet vain rikosten estämiseen ja paljastamiseen, jolloin Puolustusvoimien ei ollut mahdollista suorittaa tosiasiallisia tehtäviään (Mutanen, 2018a, s. 2).

### 4.3.2 Tiedusteluun ryhtyminen

Tiedustelumenetelmien käyttämisen päätöksenteko on porrastettu kolmivaiheiseksi, jossa päättävät tahot ovat tuomioistuin, suojelupoliisin päällikkö tai pääesikunnan tiedustelupäällikkö ja päällystöön kuuluva poliisimies tai

sotilastiedusteluviranomainen. Lisäksi ulkomaantiedustelun päätäntävalta on aina suojelupoliisin päälliköllä ja pääesikunnan tiedustelupäälliköllä. (Heikkola, 2018, s. 8.) Tuomioistuin päättää merkittävimmin perus- ja ihmisoikeuksiin puuttuvien tiedustelumenetelmien käytöstä (Laitinen, 2018b, s. 12). Tiedusteluprosessissa käytetään mahdollisesti useita tiedustelumenetelmiä. On myös erittäin vaikeaa ennalta arvioida ja osoittaa yksittäisten menetelmien tuottamien tietojen merkitystä kokonaistehtävän kannalta (HE 203/2017 vp, s. 286).

Tiedonhankinnassa aluksi saatetaan käyttää lievempiä menetelmiä ja tiedonhankinnan edetessä siirrytään käyttämään tarpeen vaatiessa enemmän perusoikeuksiin puuttuvia menetelmiä. Tilanne voi kuitenkin olla myös se, että riittävien tietojen läsnä ollessa saatetaan enemmän perusoikeuksiin puuttuvia toimivaltuuksia käyttää jo heti alussa. Käyttöä tulee kuitenkin harkita myös aina yleisten periaatteiden ja syrjimättömyyden periaatteen näkökulmasta. Merkittävä puuttuminen kohteen perusoikeuksiin jo tehtävän alkuvaiheessa voi olla perusteltua yleisten periaatteiden näkökulmasta, jos menetelmä muuten aiheuttaa vähemmän haittaa sekä kohteelle että sivullisille. Jos tiedustelun kohteena on taho, joka nauttii perusoikeussuojaa, on periaatteiden asema korostunut. Yleiset periaatteet sekä perus- ja ihmisoikeudet ovat tärkeitä periaatteita käytettäessä tiedustelumenetelmiä. Periaatteet ohjaavat tiedusteluviranomaista tarkoituksenmukaisen tiedustelumenetelmän käytössä ja varmistavat menetelmän käytön edellytysten tulkinnan pysymisen sallituissa raja-arvoissa. (HE 203/2017 vp, s. 204-205.)

Valtiolliset toimijat eivät kuitenkaan nauti perusoikeutena suojatuista oikeuksista (Lavapuro, 2018, s. 6). Meriniemen (2018) mukaan tiedustelumenetelmän kohdistuessa valtiolliseen toimijaan tai siihen rinnastettavaan tahoon, sovelletaan menetelmän käytön edellytyksiin perusteltua tuloksellisuusodotusta riippumatta käytettävästä tiedustelumenetelmästä. Tämä määrittely johdetaan siitä, että perustuslain mukaisesti valtio ei nauti perusoikeussuojaa. (Meriniemi, 2018a, s. 10.)

Siviilitiedustelussa toiminnat, jotka vakavasti uhkaavat kansallista turvallisuutta, on määritelty poliisilain 5 a luvun 3 §:ssä. Tiedustelumenetelmiä voidaan käyttää, jos tiedossa on jokin listassa mainittu toiminta. Tiedossa on kuitenkin oltava uhkan olemassaolo ja tieto uhkan tapauskohtaisista tosiseikoista. Tiedustelumenetelmille on lisäksi määritelty tietyt edellytykset päätöksentekopykälissä. Ilman todistettavia tosiseikkoja tiedusteluun ei voida ryhtyä. Se, että jokin taho antaa tiedusteluviranomaiselle tai viranomainen antaa itselleen tehtävän, ei sivuuta sitä, että uhkatiedon olemassaoloa ja uhkan tosiseikkoja ei tarvitse esittää lain määrittämällä tavalla. (Meriniemi, 2018d, s. 53.)

Tiedustelumenetelmän käytön tulee aina olla kohdennettua, jota rajaa sotilastiedustelun tarkoitus, eli sotilastiedustelu sidotaan puolustusvoimista annetussa laissa määriteltyihin Puolustusvoimien tehtäviin. Lisäksi kohdentamista rajataan ns. painopisteillä, jotka määritellään tasavallan presidentin sekä valtioneuvoston ulko- ja turvallisuuspoliittisen ministeriövaliokunnan valmisteluissa (TP-UTVA). Pääesikunnan tiedustelupäällikkö laatii painopisteiden perusteella tiedustelutehtävät, joita sotilastiedusteluviranomaiset suorittavat operatiivisella

tasalla. Operatiivisen tasan tiedustelumenetelmiä kohdennetaan edelleen menetelmien käytön yleisillä ja erityisillä edellytyksillä. (Nordström, 2018b, s. 4-5.)

Lisäksi viranomaisten toimintaa säädellään yleisesti laissa. Julkisen vallan käytön tulee aina perustua lakiin ja valtionhallinnon toimielinten yleisistä perusteista on säädettävä lailla, jos julkisen vallan käyttö tulee niiden tehtävissä kysymykseen (Rytkölä, 2018, s. 2). Myös Mickelsson (2018) toteaa, että demokraattisessa yhteiskunnassa turvallisuuden takaamiseksi suoritettujen viranomaisten tehtävien on perustuttava lainsäädäntöön (Mickelsson, 2018, s. 1).

### 4.3.3 Tiedustelumenetelmien käytön edellytykset

Siviilitiedustelua on mahdollista kohdistaa vain sellaiseen toimintaan, joka on määritelty tyhjentävästi perusteuhkana ja edellytyksenä on, että tiedustelun kohteen toiminta vakavasti uhkaa kansallista turvallisuutta. (Pelttari, 2018b, s. 4). Poliisilain 5 a luvun toimivaltuudet, jotka puuttuvat perustuslaissa 10 §:ssä 2 momentissa turvattuun luottamuksellisen viestin salaisuuteen, ovat telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, tekninen kuuntelu ja lähetyksen jäljentäminen. (Laitinen, 2018b, s. 11; ks. myös Mäenpää, 2018, s.1 ja Mutanen, 2018c, s. 5.) Vastaavat toimivaltuudet on määritelty myös sotilastiedustelun osalta (Meriniemi, 2018a, s. 7).

Tiedustelumenetelmien käytön edellytykset on säädetty poliisilain 5 a luvun 4 §:ssä ja sotilastiedustelulain 12 §:ssä seuraavasti (1. virke):

> Tiedustelumenetelmän käytön yleisenä edellytyksenä siviilitiedustelussa on, että sen käyttäminen on välttämätöntä tärkeiden tietojen saamiseksi sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. (Poliisilaki, 5 a luku, 2019.)

> Tiedustelumenetelmän käytön yleisenä edellytyksenä on, että tiedustelumenetelmän käyttö on välttämätöntä ja että sillä voidaan perustellusti olettaa saatavan tärkeää tietoa tiedustelutehtävän kannalta. Jos tiedustelumenetelmä kohdistetaan valtiolliseen toimijaan, tiedustelumenetelmän käytön yleisenä edellytyksenä on, että tietojen saaminen on tarpeen tiedustelutehtävän kannalta. (Laki sotilastiedustelusta, 2019.)

Lisäksi laeissa jäljempänä on säädetty erityisistä edellytyksistä. Telekuuntelua ja tietojen hankkimista telekuuntelun sijasta, suunnitelmallista tarkkailua, teknistä kuuntelua, teknistä katselua, henkilön teknistä seurantaa, teknistä laitetarkkailua, peitetoimintaa, valeostoa, tietolähteen ohjattua käyttöä ja paikkatiedustelua saadaan siviilitiedustelussa käyttää vain perusteltuna. Käyttö on mahdollista, kun perusteltu oletus erittäin tärkeästä merkityksestä tietojen saamiseksi täyttyy. Jos menetelmän käyttämisen välttämättömyysedellytys täytyy, voidaan käyttää myös peitetoimintaa ja valeostoa. Peitetoiminnasta on lisäksi määritelty, että tiedonhankinnan on oltava tarpeellista, koska kohteena oleva toiminta on suunnitelmallista, järjestäytynyttä, ammattimaista, jatkuvaa tai toistuvaa. (Meriniemi, 2018a, s. 8.)

Tiedustelumenetelmien käytön edellytyksiä ei tosiasiallisesti ole mahdollista porrastaa, kuten salaisten tiedonhankintakeinojen ja pakkokeinojen käytön edellytyksiä porrastetaan poliisi- ja pakkokeinolaissa, koska tiedustelutoiminnassa kohteena eivät ole rikokset (Mutanen, 2018c, s. 6).

Tiedonhankintaa voidaan kohdistaa myös yksilön sijasta ryhmään. Tätä perustellaan tiedustelutoiminnan osalta sillä, että toimivaltuuksilla voi olla tarve saada tietoa henkilöryhmän koko organisaatiosta, ryhmän henkilöistä ja ryhmän aktiivisuudesta tietyllä alueella sekä ryhmään yhdistetystä toiminnasta ja sen muodoista. (Meriniemi, 2018b, s. 50.)

Ylemmät laillisuusvalvojat ovat ratkaisukäytännöissään todenneet, että tehtävämäärittelyä koskevat säännökset eivät ole toimivaltasäännöksiä. Ratkaisukäytäntöjä ovat esimerkiksi eduskunnan apulaisoikeusasiamiehen päätökset 29.11.2013 dnro 1870/2013 ja 18.12.2003 dnro 1634/4/01. Tehtäväsäännös ei anna toimivaltaa ryhtyä tehtävien suorittamiseksi millaisiin toimiin tahansa, eikä pelkästään sen perusteella voida puuttua ihmisten lainsäädännöllä suojattuihin oikeuksiin. Oikeuspiiriin puututtaessa toimivallan on perustuttava nimenomaiseen säännökseen. Kansallisen turvallisuuden suojaaminen ei näin ollen itsessään osoita muuta kuin sen, että tiedustelulla on lainmukainen ja yhteiskunnallisesti toivottava motiivi menettelylle. Tämä ei yksinään oikeuta puuttumaan ihmisten perusoikeuksiin, vaan toimivaltaperuste tulee löytyä laista. (HE 202/2017 vp, s. 70.) Meriniemi (2018) on lisäksi todennut, että valtaa ei voida käyttää tehtävän näennäiseen suorittamiseen, johon vallankäyttö voisi sinänsä sopia ja oikeasti tavoitteena on luoda toimivalta toiseen toimenpiteeseen, johon käsittelyssä olevia valtuuksia ei ole oikeutta liittää (Meriniemi, 2018d, s. 4).

Kaikille tiedustelumenetelmille yhteisten käyttöedellytysten perusteella täytyy voida perustellusti olettaa, että tiedustelulla saadaan tietoja sellaisesta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Kyseessä on tuloksellisuusvaatimus ja perusteltu hyödyllisyys, joka on tiedustelumenetelmän käytön odotusarvona. Ilmaisu ”perustellusti” tarkoittaa sitä, että tiedustelumenetelmän käytön hyödyllisyys tulee kyetä perustelemaan yksittäistapauksellisesti. Perustelulla tarkoitetaan esimerkiksi sitä, että kerrotaan, kuinka tiettyä henkilöä tai henkilöryhmää tarkkailemalla saadaan oletetusti hyödyllistä tietoa kansallisen turvallisuuden kannalta. Tämä taas liittyisi esimerkiksi siihen, kuinka havaintojen mukaan tietty henkilö tai henkilöryhmä on käyttäytynyt. (HE 202/2017 vp, s. 177; Laitinen, 2018b, s. 10.)

Laitinen (2018) myös toteaa, että pelkästään tiedustelun kohde ei yksinään mahdollista tiedustelumenetelmien käyttöä, vaan menetelmän käytön lähtökohtana on oltava ns. perusteltu hyödyllisyys ja kyse on perustelua edellyttävästä tuloksellisuusvaatimuksesta. Menetelmille on määritelty yhteinen yleinen käyttöedellytys, jonka mukaan tulee voida perustellusti olettaa, että menetelmän käytöllä saadaan tietoja kohteena olevasta toiminnasta, joka uhkaa kansallista turvallisuutta vakavasti. (Laitinen, 2018b, s. 9.)

Hakosen (2018) mukaan tiedustelun tulee tietysti olla lainmukaista, mutta sen lisäksi tiedustelun tulee täyttää tehokkuuden ja tarkoituksenmukaisuuden vaatimukset. Toimintaympäristö on muutoksessa, jolloin Hakosen mukaan

tehokkuusvaatimus sekä tietojen hankkiminen ja analysointi voi muodostua lainmukaisuutta haastavammaksi. (Hakonen, 2018b, s. 3.)

## 4.4 Avoimet lähteet tiedustelussa

HE 203/2017 vp:n mukaan OSINT ei loukkaa kohteen yksityisyyden suojaa tai luottamuksellisen viestin salaisuutta, jolloin erityistä säädösperustaa ei OSINT:lle tarvita (HE 203/2017 vp, s. 89). Myös Vainio (2018) toteaa, että osaa tiedustelumenetelmistä voidaan käyttää ilman tarkempia edellytyksiä, jolloin menetelmä ei rajoita yksityisyyttä tai kohdistuu valtiolliseen toimijaan (Vainio, 2018, s. 7). Näin ollen aiemmissa luvuissa esitetyt edellytykset tiedustelumenetelmien käytöllä eivät avointen lähteiden tiedustelua suurimmilta osin koske.

Lainsäädäntö on mahdollistanut jo ennen tiedustelulainsäädäntöä avointen lähteiden tiedustelun sekä lisäksi radiosignaalitiedustelun, kuvaustiedustelun ja henkilötiedustelun tietyissä tilanteissa (HE 203/2017 vp, s. 20). Hallituksen esityksessä HE 203/2017 vp myös todetaan, että ennen tiedustelulainsäädäntöä tiedustelu on perustunut pitkälti julkisiin lähteisiin ja yhteistyöhön muiden tahojen kanssa (HE 203/2017 vp, s. 6). Tiedustelulainsäädännön voimaantulon myötä avointen lähteiden tiedustelun rooli on todennäköisesti kaventunut ja tietotarpeita kyetään täyttämään muilla menetelmillä, mitä aiemmin ei ole ollut mahdollista tehdä. Lisäksi tiedustelutoiminnassa ei tarvitse enää nojata niin paljon yhteistyökumppaneiden tietoihin.

Aapion (2018) mukaan suojelupoliisi käyttää yleisesti toiminnassaan avoimia lähteitä ja kaikkia tai useita keinoja voidaan käyttää myös samassa asiassa (Aapio, 2018, s. 3). Ennen tiedustelusääntelyä salaisten tiedonhankintakeinojen käyttöperusteet oli määritelty henkilö- ja rikoslähtöisesti. Näin ollen ilman rikostorjunnallista perustetta salaisia tiedonhankintakeinoja ei ole voinut käyttää. Myös Puolustusvoimien on tällöin ollut pakko nojata avointen lähteiden seurantaan ja yhteistyöverkon kautta saatuihin tietoihin. (HE 203/2017 vp, s. 23.) Aiemmin myös Puolustusvoimien ulkomaita koskeva tiedonsaanti on nojannut käytännössä kansainväliseen yhteistyöhön, puolustusasiamiestoimintaan ja avointen lähteiden seurantaan (HE 203/2017 vp, s. 36).

Melaluoto on (2018) todennut, että pelkästään avoimiin lähteisiin ja kansainväliseen tietojenvaihtoon nojaava tiedustelutoiminta ei nykyisen turvallisuustoimintaympäristön näkökulmasta ole kuitenkaan riittävää (Melaluoto, 2018, s. 3).

### 4.4.1 Verrokkimaat

Hallituksen esityksessä HE 203/2017 vp on esitelty myös verrokkimaiden tiedonhankintaa. HE:n mukaan Tanskassa laki ei erottele tiedustelupalvelun tiedustelumenetelmiä, mutta tietojen hankinnassa hyödynnetään yleisesti myös avoimia lähteitä (HE 203/2017 vp, s. 71).

Alankomaissa taas tiedustelun erityiset toimivaltuudet on sidottu tiettyihin periaatteisiin, joiden mukaan julkisia lähteitä tai muussa virastossa olevaa tietoa on käytettävä ensisijaisesti (HE 203/2017 vp, s. 80).

Sveitsissä taas lain mukaan tiedustelupalvelu voi ilman erillistä lupaa käyttää julkisia tietolähteitä, kuten mediaa, yksityisten julkiseksi asettamia tietoja, valtion viranomaisten julkisia rekistereitä ja julkisuudessa esitettyjä lausumia (HE 203/2017 vp, s. 84). Lisäksi Sveitsissä tiedustelupalvelu voi ilman erillistä lupaa lain mukaan käyttää henkilöitä tietolähteinä, ilmoittaa henkilöitä ja ajoneuvoja poliisin etsintäkuulutusjärjestelmään sekä tarkkailla ja nauhoittaa kuvaa ja ääntä julkiseksi määritellyissä tiloissa (HE 203/2017 vp, s. 84).

Myös esimerkiksi Venäjällä FSB:llä ja sisäministeriöllä on käytössään ”Semanttinen arkisto”, jota käytetään avointen lähteiden, kuten median, blogien, Internetin ja SOME:n seurantaan (Lehto, 2018, s. 18).

### 4.4.2 Sääntelemättömyys

Sotilastiedusteluviranomaisilla on käytössään myös tiedonhankintakeinoja, jotka eivät vaadi erityistä toimivaltuussääntelyä. Tällaisiin keinoihin lasketaan kuvaustiedustelu, geotiedustelu ja avointen lähteiden tiedustelu. Näissä tapauksissa on kyse tiedonhankinnasta, jonka ei katsota loukkaavan yksityisyyden suojaa. Näin ollen avointen lähteiden tiedustelusta ei perustuslain mukaan tarvitse lailla säätää. (HE 203/2017 vp, s. 218.) Siviiliviranomaisten tiedonhankinta perustui ennen tiedustelulainsäädäntöä rikostorjuntatoimivaltuuksiin, julkisiin lähteisiin, kansainvälisen ja muun yhteistyön, kuten vapaaehtoisen yhteistyön avulla saataviin tietoihin (HE 202/2017 vp, s. 6). Hallituksen esityksessä HE 202/2017 vp todetaan, että tiedustelutiedon hankinta avoimista lähteistä on ollut mahdollista myös ennen tiedustelulainsäädäntöä (HE 202/2017 vp, s. 19). Näin ollen aiemmat rikosperusteisuuteen perustuvat toimivaltuudet eivät myöskään ole avointen lähteiden tiedustelua rajoittaneet.

Hallituksen esityksen HE 202/2017 vp:n mukaan julkisesti saatavilla olevaa tietoa voidaan kerätä vapaasti, eikä tiedonhankinnan tarvitse perustua erikseen säädettyyn viranomaistoimivaltuuteen. Tiedonhaun perustuminen pelkästään julkisesti saatavilla oleviin tietoihin, on kuitenkin hallituksen esityksen HE 202/2017 vp:n mukaan käytännössä mahdotonta. Suojelupoliisi torjuu sellaisia hankkeita ja rikoksia, joita pääsääntöisesti valmistellaan salassa, josta on keskeistä saada tietoa myös muuten, kuin julkisista lähteistä. Lisäksi hallituksen esityksen mukaan tiedonhankinta voi olla tehokasta vain, jos sitä suoritetaan salassa sen kohteelta. Irtautuminen rikosperusteisista toimivaltuuksista antaa suojelupoliisille mahdollisuuden käyttää toimivaltuuksiaan valtion turvallisuuteen liittyvän uhkatiedon hankkimiseksi. (HE 202/2017 vp, s. 16.) Myös hallituksen esityksen HE 203/2017 vp:n mukaan erikseen säädettyä viranomaistoimivaltuutta ei edellytetä julkisesti saatavilla olevan tiedon hankkimiseksi (HE 203/2017 vp, s. 20). Kuten siviilitiedustelun kohdalla, myös Puolustusvoimien torjuttavina olevat rikokset ja hankkeet valmistellaan usein salassa, jolloin julkisesti saatavilla olevat tiedot eivät yksinään riitä. Keskeistä on, että saadaan tietoa toiminnasta,

jota tehdään salassa ja tehokkuuden vuoksi myös tiedonhankinta on kyettävä toteuttamaan salassa. (HE 203/2017 vp, s. 20.)

Ennen tiedustelulainsäädäntöä suojelupoliisin ulkomaita koskeva tiedonhankinta on nojannut kansainväliseen tiedusteluyhteistyöhön, avointen lähteiden seurantaan sekä suojelupoliisin omaan yhdysmiestoimintaan (HE 202/2017 vp, s. 33). Tiedustelulainsäädäntö mahdollistaa nykyään laajemmat toimivaltuudet, jolloin avointen lähteiden tiedustelun rooli on mahdollisesti kaventunut ja muuttunut enemmän tukevaksi tiedustelumenetelmäksi. Näin myös todetaan hallituksen esityksessä. SUPO:n ulkomaita koskeva avointen lähteiden seuranta kattaa koko viraston toimialan ja avoimista lähteistä saadut tiedot yhdistetään muiden lähteiden tietoihin tilannekuvan muodostamiseksi kansainvälisestä turvallisuusympäristöstä (HE 202/2017 vp, s. 34).

Ennen tiedustelulainsäädäntöä tiedonhankinnan kohteena oleva henkilö on pitänyt kyetä yksilöimään vähintäänkin henkilön roolin tai tehtävän perusteella. Näin on ollut myös tilanteessa, jossa kohde on ollut henkilöllisyydeltään ennestään tuntematon. Telekuuntelua ja televalvontaa on voitu kohdistaa tuntemattomaan henkilöön, mutta perusteena on täytynyt esittää esimerkiksi IP-osoite tai IMEI-koodi. Ilman tällaista rikostorjunnallista perustetta salaisia tiedonhankintakeinoja ei ole ollut mahdollista käyttää. Tällöin tiedustelu on ollut vahvasti avointen lähteiden, poliisin yleisvalvonnan ja yhteistyötoiminnan varassa. (HE 202/2017, vp, s. 73.)

### 4.4.3 Tiedonhankinnan kohteet

Hallituksen esityksen HE 203/2017 vp:n mukaan avointen lähteiden tiedustelutieto on tietämystä, joka perustuu avoimista lähteistä hankittuun informaatioon ja se on yhdenmukaisesti jaoteltu, arvioitu ja suodatettu. Informaatio koostuu tiedoista, joita jokainen kansalaisen voisi laillisesti itse pyytää tai havainnoida. Tyypillisesti HE:n mukaan tietolähteitä ovat kirjallisuus, kartat, lehdet, tilastot, julkaisut, yleisölle suunnatut televisio- ja radiolähetykset sekä SOME-sisällöt. Tiedonhankinta voidaan OSINT:ssa jakaa joko rajattuun tiedustelukysymykseen perustuvaan tiedonhankintaan tai mediaseurantaan. Mediaseurannassa tarkoituksena on lähinnä tiedustelutilannekuvan tukeminen. HE:n mukaan OSINT:ssa tiedonhankinta kohdistuu lähinnä laajempien ilmiöiden ja tapahtumien yhteyteen. Lisäksi on erikseen mainittu, että pitkäkestoista tiedonhankintaa ja seurantaa kohdistetaan myös esimerkiksi yksittäiseen sosiaalisen median tiliin. Tätä pidetään tärkeänä tietyn tapahtuman ymmärtämiseksi tai tiedon luotettavuuden arvioimiseksi. Viimeisten vuosien aikana sosiaalinen media on muutenkin tunnistettu arvokkaaksi, jolloin SOME:n kautta saatavien havaintojen määrä on suhteessa muihin lähteisiin kasvanut merkittävästi. OSINT:iin ei HE:n mukaan sisälly ns. aktiivista osallistumista, jolla tarkoitetaan esimerkiksi tietoverkoissa käytävään keskusteluun osallistumista tiedon saamiseksi. Tietoa voidaan lisäksi hankkia myös ostamalla tai kolmansien osapuolien avulla. OSINT:ia suoritetaan joko yksinään tai muiden tiedustelumenetelmien tukena. OSINT:ia käytetään yksinään erityisesti silloin, kun muiden menetelmien käyttö ei ole tehokasta tai

mahdollista. Avointen lähteiden osalta tiedostetaan se, että tietoa on saatavilla valtavasti ja väärien tietojen mahdollisuus on suuri. OSINT:n vahvuuksiin kuuluu HE:n mukaan mm. sen nopeus, maantieteellinen rajoittamattomuus, edullisuus ja mahdollisuus kerätä tietoja myös tulevista tapahtumista. HE:n mukaan lisäksi pelkästään OSINT:n keinoin tuotettu tiedustelutuote on tyypillisesti suojaustasoltaan muita tiedustelutuotteita julkisempi, minkä ansioista OSINT-tuotteen käytettävyys on parempi. (HE 203/2017 vp, s. 33.)

Lisäksi OSINT:lla tarkoitetaan myös esimerkiksi tiedon hankintaa julkisista tiedotusvälineistä, julkisista viranomaisrekistereistä, julkisista tietokannoista ja julkisuudessa avoimesta esitetyistä lausumista (HE 203/2017 vp, s. 218). Internet käsitetään OSINT:ssa omana kanavanaan tiedon hankkimiseksi, eikä niinkään omana tiedonlähteenään (HE 203/2017 vp, s. 218).

Kaila (2018) toteaa tietoverkoissa olevista tiedoista, että kansalaisten sekä julkisyhteisöjen julkisia ja ei-julkisia tietoja kerätään ja hyödynnetään kansainvälisesti, kaupallisesti ja muihin tarkoituksiin ja myös henkilötiedot ovat hänen mukaansa arvokasta kauppatavaraa (Kaila, 2018a, s. 3).

Lehto taas on (2018) asiantuntijalausunnossaan esitellyt Googlen toimintaa tietojen keräämisessä. Lataamalla, lähettämällä tai tallentamalla sisältöä palveluihin annetaan Googlelle ja sen yhteistyökumppaneille maailmanlaajuinen oikeus käyttää, ylläpitää, tallentaa, jäljentää, muokata, välittää, julkaista, esittää ja levittää kyseistä sisältöä sekä asettaa sitä julkisesti esille. Kyseinen käyttöoikeus myös pysyy voimassa, vaikka palvelujen käyttö lopetettaisiin, tiedoilla tarkoitetaan esimerkiksi yritystietoja, joita ladataan Google Mapsiin. (Lehto, 2018, s. 29). Tämä lausunto osaltaan osoittaa sitä, kuinka paljon ja minkälaisia tietoja tietoverkoista on mahdollista löytää ja käyttää hyväksi toisaalta tiedustelutoiminnassa, mutta toisaalta myös muiden tahojen toimesta.

HE 202/2017 vp:n mukaan tiedustelutietoa saadaan useista lähteistä, joita ovat avoimet lähteet, oma operatiivinen toiminta, kotimaiset yhteistyökumppanit sekä ulkomaiset turvallisuus- ja tiedusteluviranomaiset. Tiedustelutehtävien toteuttaminen vaatii laaja-alaista ja aktiivista turvallisuusympäristön seuraamista ja ennakoivaa tiedonhankintaa. (HE 202/2017 vp, s. 14.)

Hallituksen esityksessä 203/2017 vp on myös maininta OSINT:n hyödyntämisestä tietoliikennetiedustelussa. Teknisten tietojen käsittelyllä pyritään rajaamaan tietoliikennetiedustelussa epärelevantti tietoliikenne jo heti alkuvaiheessa. Viestinnän teknisiä tietoja käsittelemällä pyritään selvittämään, missä viestintäverkon osassa tietyn toimijan tai tietyn maantieteellisen alueen tietoliikenne kulkee. Tässä vaiheessa voidaan esimerkiksi hankkia julkisista lähteistä tietoa BGP-reitityksestä, joka kertoo niiden autonomisten järjestelmien omistajat, joiden kautta viesti on tiettyyn pisteeseen tullut. Kyseisten järjestelmien omistajat ovat esimerkiksi operaattoreita, jotka vastaavat tietyn IP-osoitealueen reitittämiskokonaisuudesta. (HE 203/2017 vp, s. 277.) Kaila (2018) on tähän liittyen todennut, että tietyt avoimesti saatavilla olevat tiedot ja niiden kerääminen laillista ja valvottua tiedustelutoimintaa varten tulee olla lainsäädännössä sallittua. Tällaisia avoimesti saatavilla olevia tietoja ovat mm. kohde- ja lähdeosoitteet, käytetyt protokollat, otsikkotiedot yleensäkin, liikennemäärät ja nimipalvelukyselyt.

Lisäksi salaamattoman tietoliikenteen sisältö, esimerkiksi salaamaton selainliikenne ja salaamattomat puhelut, videoneuvottelut sekä sähköpostit. Lisäksi Kaila mainitsee myös, että palvelinten ja aktiivi- sekä päätelaitteiden haavoittuvuuksien havaitsemisen tulee olla sallittua, kuten myös haavoittuvuuksien tunnistetietojen keräämisen. Haavoittuvuuksien hyödyntämisen tulee kuitenkin edellyttää esimerkiksi peitetoiminnan mukaista lupaa. (Kaila, 2018b, s. 4.)

Kolehmainen (2018) toteaa, että tietoa on valtavasti ja tiedustelulainsäädäntö on lisännyt saatavissa olevan tiedon määrää. Kyky yhdistellä tietoja on hänen mukaansa tärkeintä, eikä kyse ole vain salaisilla tiedonhankinnalla saaduista tiedoista, vaan kaikkea saatavilla olevaa tietomassaa tulee pystyä hyödyntämään, kuten julkisia lähteitä. (Kolehmainen, 2018, s. 3.)

### 4.4.4 OSINT:n suhde toimivaltuussääntelyyn

Meriniemi (2018) toteaa, että soveltamisalasäännös säätää suojelupoliisin suorittamasta tiedonhankinnasta ja tiedon käyttämisestä kansallisen turvallisuuden suojaamiseksi. Hänen mukaansa tiedonhankinta ”ei kuitenkaan tyhjene” 5 a luvussa tarkoitettuihin tiedustelumenetelmiin, vaan tiedonhankintaa voidaan vapaasti tehdä myös avoimista lähteistä. Laajempana kokonaisuutena tiedonhankintaan kuuluu myös esimerkiksi vihjepuhelimen tai vihjesähköpostin avulla saadut tiedot. Kummatkaan edellisistä eivät Meriniemen mukaan edellytä

> ”sellaisen siviilitiedustelun kohteena olevan toiminnan osoittamista, joka muodostaa vakavan uhkan kansalliselle turvallisuudelle ja, että jonkun tietyn tiedustelumenetelmän käyttö on välttämätöntä”.

Hänen mukaansa kyse on täysin normaalista suojelupoliisin poliisitoiminnasta. Tehtäväsääntelyllä tietysti rajataan suojelupoliisin asiallista toimivaltaa, jolloin vihjepuhelin ei voi koskea esimerkiksi autokauppaa tai vastaavaa asiallisen toimivallan ulkopuolelle rajattavaa asiaa. Toiminnalla tulee aina kuitenkin näin ollen olla jokin liityntä kansallisen turvallisuuden suojaamiseen. (Meriniemi, 2018f, s. 3; ks. myös HaVM 36/2018 vp, s. 47.)

Osa tiedustelutoimivaltuuksista on myös perusoikeussuojan näkökulmasta kevyempiä. Fredman (2018) toteaakin, että tiedustelulainsäädännön tuomista toimivaltuuksista kaikki eivät kohdistu yksityiselämään tai luottamukselliseen viestintään, kuten suurimmilta osin tietojen saanti yksityiseltä yhteisöltä (Fredman, 2018, s. 1).

Tiedustelumenetelmien käytössä välttämättömyysedellytys tarkoittaa sitä, että luottamuksellisen viestin salaisuuteen kohdistuva rajoitus on sallittu, jos tiedonhankintaa ei voida toteuttaa vähemmän puuttuvalla keinolla ja tiedonhankinnassa luottamuksellisen viestin salaisuuteen puututaan niin kohdennetusti ja rajoitetusti kuin on mahdollista. Hallintovaliokunta (2018) toteaa, että siviilitiedustelutoimivaltuudet määritellään poliisilain 5 a luvussa ja tietoliikennetiedustelua käsittelevässä laissa, jolloin myös näistä löytyvät kaikki käytettävissä olevat toimivaltuudet. Tämä tulee ottaa huomioon välttämättömyysedellytystä arvioitaessa, sillä välttämätöntä on käyttää lakiin perustuvaa

tiedustelumenetelmää siviilitiedustelussa. Muita tiedustelumenetelmiä ei käytännössä avointen lähteiden lisäksi ole käytettävissä. Valiokunta on myös todennut, että tilannekohtaisesti usein ei ole käytettävissä vaihtoehtoisia tiedustelumenetelmiä, vaan esimerkiksi tietoliikenteeseen kohdistuvaan uhkaan on käytettävä tietoliikennetiedustelua. (HaVM 36/2018 vp, s. 32.)

Hallituksen esityksessä HE 203/2017 vp on pohdittu luottamuksellista viestintää. Tästä pohdinnasta voidaan tehdä johtopäätöksiä myös tarkkailuun ja toisaalta avointen lähteiden tiedusteluun liittyen. HE:n mukaan luottamuksellista viestintää on käsitelty useissa lausunnoissa, kuten HE 309/1993 vp, s. 53, PeVL 11/2005 vp, s. 4, PeVL 36/2002 vp,s. 6, PeVL 2/1996 vp ja PeVL 5/1999 vp, s. 4. Luottamukselliseksi tarkoitetun keskustelun kuunteleminen teknisellä apuvälineellä merkitsee väistämättä rajoitusta luottamuksellisen viestin salaisuuden suojaan. Säännös ei kuitenkaan suojaa tavallista kuuloetäisyydellä käytävää keskustelua, jota on mahdollista aistihavainnoin havaita. Kyse on tällöin tiedoista, joita kuka tahansa voi itse havaita. Luonnollisia henkilöitä ja oikeushenkilöitä suojataan perusoikeussäännöksillä välillisesti, mutta valtiot ja muut ns. julkisyhteisöt eivät nauti perusoikeussuojaa. Näin ollen myöskään vieraan valtion viranomaisorganisaation viestintä ei kuulu luottamuksellisen viestin salaisuuden suojan soveltamisalaan. (HE 203/2017 vp, s. 349.)

## 4.5 Peitetaktiikat ja tarkkailu tietoverkoissa

Tässä luvussa käsitellään aineistosta nousseita näkökulmia liittyen tarkkailutyyppisiin menetelmiin ja peitetaktiikoihin. Menetelmistä on löydettävissä yhteyksiä myös OSINT:iin ja näin ollen myös tutkimusongelmaan.

### 4.5.1 Tarkkailu

Poliisilain 5 luvun 13 §:n 1 momentissa säädetään niin sanotusta tarkkailun yleismääritelmästä seuraavasti:

> 13 §
>
> Suunnitelmallinen tarkkailu ja sen edellytykset
>
> Tarkkailulla tarkoitetaan tiettyyn henkilöön salaa kohdistettavaa havaintojen tekemistä tiedonhankintatarkoituksessa. Tarkkailussa voidaan rikoslain 24 luvun 6 §:n estämättä käyttää näköhavaintojen tekemiseen tai tallentamiseen kameraa tai muuta sellaista teknistä laitetta. (30.12.2013/1168) (Poliisilaki.)

Yleismääritelmän mukaan tarkkailulla tarkoitetaan tiettyyn henkilöön kohdistettavaa havaintojen tekemistä tiedon hankkimiseksi salassa. Lisäksi saman 13 §:n 4 momentissa sanotaan:

> Tässä pykälässä tarkoitettua tarkkailua ei saa kohdistaa vakituiseen asumiseen käytettävään tilaan. Teknistä laitetta ei saa käyttää rikoslain 24 luvun 11 §:ssä tarkoitettuun kotirauhan suojaamaan paikkaan kohdistuvassa tarkkailussa tai suunnitelmallisessa tarkkailussa. (30.12.2013/1168) (Poliisilaki.)

Tarkkailua ei siis saa kohdistaa vakituiseen asumiseen käytettävään tilaan, mutta aistinvarainen tarkkailu, jonka tavoitteena on rikoksen estäminen ja paljastaminen, on kuitenkin sallittua kohdistaa myös kotirauhan piirissä olevaan henkilöön (HE 202/2017 vp, s. 23.)

HE 203/2017 vp:ssä todetaan, että tarkkailu ei ennen tiedustelusääntelyä ole soveltunut uhkien havaitsemiseen, mutta jo esityksessä todettiin, että tarkkailua voitaisiin käyttää myös tiedustelumenetelmänä hankkimaan tietoa toiminnasta, joka luonteeltaan on sotilaallista tai vakavasti kansallista turvallisuutta uhkaavaa (HE 203/2017 vp, s. 96).

Tarkkailutyyppisten keinojen avulla saatuja tietoja voidaan käyttää tiedustelun vaikuttavuuden tehostamiseen. Näillä keinoilla saaduilla reaaliaikaisilla tiedoilla on mahdollista parantaa merkittävästi tilannekuvaa ja samalla helpottaa myös päätöksentekoa tiedustelun suuntaamiseen ja painopisteisiin liittyen. (HE 203/2017 vp, s. 98.) Tarkkailusta ja suunnitelmallisesta tarkkailusta säädetään sotilastiedustelulain 22 §:ssä seuraavasti:

> 22 §
>
> Tarkkailu ja suunnitelmallinen tarkkailu
>
> Tarkkailulla tarkoitetaan tiettyyn henkilöön tai, jos tiettyä henkilöä ei voida yksilöidä, henkilöryhmään salaa kohdistettavaa havaintojen tekemistä tiedustelutarkoituksessa. Tarkkailussa voidaan rikoslain 24 luvun 6 §:n estämättä käyttää näköhavaintojen tekemiseen tai tallentamiseen kameraa tai muuta sellaista teknistä laitetta.
>
> Suunnitelmallisella tarkkailulla tarkoitetaan muun kuin lyhytaikaisen tarkkailun kohdistamista henkilöön tai henkilöryhmään, jonka voidaan perustellusti olettaa liittyvän tiedustelutehtävään. (Laki sotilastiedustelusta, 2019.)

Tarkkailunkin osalta on korostettu yleisten periaatteiden huomioimista ja tarkkailua voidaan kohdistaa henkilöön sekä henkilöryhmään. Toimenpiteelle tyypillistä on, että havaintoja tehdään huomaamattomasti. Tarkkailua voidaan HE:n mukaan toteuttaa siten, että tiedonhankinnan kohde ei havaitse olevansa kohteena, vaikka kuitenkin varsinainen havainnointi tehdäänkin täysin avoimesti. Kysymykseen tarkkailun osalta tuleekin, että havainnot tehdään salaa sekä havaintojen tekeminen salaten myös tiedonhankintatarkoitus. (HE 203/2017 vp, s. 221.)

Internetiä koskevan tarkkailun osalta vallitsee käsitys, jonka mukaan erityistä toimivaltuussääntelyä ei tähän tarvita. Tämä pätee silloin, kun tarkkailua suoritetaan yleisissä tietoverkoissa, esimerkiksi keskustelupalstoilla. Tätä ei myöskään sotilastiedustelulakiesityksessä ehdotettu muutettavaksi. Tietoverkoissa tapahtuvaa tarkkailua määritellään passiiviseksi ihmisten väliseen

vuorovaikutukseen kohdistuvaa tiedonhankintaa, kuten muutenkin tarkkailua suoritetaan. Lisäksi esimerkiksi tietyn rakennuksen, tilan tai keskustelupalstan tarkkailu ei ole varsinaisen tarkkailutoimivaltuuden käyttöä. Tällaisesta tarkkailusta ei avointen lähteiden tiedustelun tavoin ole tarpeellista erikseen säätää laissa. Teknisestä tarkkailusta puhutaan silloin, kun käytetään tiettyyn paikkaan sijoitettua teknistä laitetta, menetelmää tai ohjelmistoa. Näin ollen esimerkiksi kiikarin tai kameran käyttö tarkkailussa ei muuta toimenpiteen luonnetta aistein tehtäviin havaintoihin verrattuna. (HE 203/2017 vp, s. 95.)

Tietoverkoissa tapahtuvassa tarkkailussa saatetaan myös tarvita toisen valtion virkamiehen apua, jolla olisi puuttuva ominaisuus tai osaaminen, kuten esimerkiksi kielitaito tai kulttuurillinen tuntemus. Vastaavanlaista menettelyä voidaan tarvita tarkkailun lisäksi myös peitellyssä tiedonhankinnassa ja peitetoiminnassa. Lisäksi vieraan valtion tiedustelupalvelun virkamiehellä voi olla arvokkaita tietolähteitä tiedustelutehtävän kannalta. (Meriniemi, 2018e, s. 39.)

### 4.5.2 Peitelty tiedonhankinta

Poliisilain 5 luvun 15 §:ssä säädetään peitellystä tiedonhankinnasta seuraavasti:

> 15 §
>
> Peitelty tiedonhankinta ja sen edellytykset
>
> Peitellyllä tiedonhankinnalla tarkoitetaan tiettyyn henkilöön kohdistuvaa lyhytkestoisessa vuorovaikutuksessa tapahtuvaa tiedonhankintaa, jossa poliisimiehen tehtävän salaamiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja.

Peitellyssä tiedonhankinnassa luonteenomaista on pyrkiä henkilökohtaiseen tapaamiseen tai muuhun vuorovaikutukseen kohteen kanssa, joka samalla erottaa menetelmän myös tarkkailusta ja suunnitelmallisesta tarkkailusta. Peitellyssä tiedonhankinnassa ei kuitenkaan ole peitetoiminnan tavoin kyse soluttautumisesta, jonka tavoitteena on rakentaa pitkäaikainen luottamussuhde kohteeseen. Peitellyssä tiedonhankinnassa voidaan myös pykälän mukaisesti käyttää vääriä, harhauttavia tai peiteltyjä tietoja, jotta tiedonhankinnan paljastuminen on mahdollista estää. (HE 202/2017 vp, s. 23.)

HE 203/2017 vp:n mukaan peitelty tiedonhankinta sijoittuu suunnitelmallisen tarkkailun ja peitetoiminnan välimaastoon. Esityksen mukaan menetelmässä on selkeitä peitetoiminnan piirteitä, mutta toiminnassa ei pyritä luottamussuhteen luomiseen. Tiedustelutoiminnassa peitellyssä tiedonhankinnassa voi olla tarve kohdistaa menetelmää myös henkilöryhmään. (HE 203/2017 vp, s. 96.) Poliisilain 5 a luvun 9 §:n 3 momentissa on esitetty henkilöryhmän määritelmä seuraavasti:

> Henkilöryhmällä tarkoitetaan tässä laissa vähintään kolmen hengen muodostamaa tietyn ajan koossa pysyvää ja rakenteeltaan jäsentynyttä yhteenliittymää, joka toimii yhteistuumin tai yhteisen tavoitteen saavuttamiseksi. (Poliisilaki, 5 a luku.)

Peitellystä tiedonhankinnasta säädetään sotilastiedustelulain 24 §:ssä seuraavasti:

> 24 §
>
> Peitelty tiedonhankinta
>
> Peitellyllä tiedonhankinnalla tarkoitetaan tiettyyn henkilöön tai, jos tiettyä henkilöä ei voida yksilöidä, henkilöryhmään kohdistuvaa lyhytkestoisessa vuorovaikutuksessa tapahtuvaa tiedonhankintaa, jossa sotilastiedusteluviranomaisen virkamiehen tehtävän salaamiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja.
>
> Sotilastiedusteluviranomainen saa käyttää peiteltyä tiedonhankintaa tiedustelutehtävän suorittamiseksi. (Laki sotilastiedustelusta, 2019.)

Sotilastiedustelua koskevassa lakiesityksessä peiteltyä tiedonhankintaa havainnollistetaan siten, että esimerkiksi arkipäiväisessä tilanteessa tiedustelun kohteelta kysytään matkakohteesta tai kielitaidosta siten, ettei tehtävää suorittava virkamies paljasta omaa henkilöllisyyttään. Toisena esimerkkinä on mainittu tilanne, jossa kohteelle voidaan toimittaa hänelle tarkoitettu lähetys, esiintyen kyseisenä lähettinä. Peitellylle tiedonhankinnalle ei ole mielekästä asettaa tiettyä aikarajaa, koska esimerkiksi kohde voi pitkittää tilannetta ja epäluotettava turhan äkkipikainen irtaantuminen tilanteesta voisi vaarantaa tehtävän. (HE 203/2017 vp, s. 227.)

HE:n mukaan peiteltyä tiedonhankintaa voidaan suorittaa myös tietoverkoissa. Tällöin kuitenkin täytyy kiinnittää huomiota siihen, että tehdään riittävä rajanveto peitetoimintaan nähden. Myös tietoverkoissa kyse on lyhytkestoisesta vuorovaikutuksesta, jossa tietoa pyritään hankkimaan. Tällainen tilanne voi tulla esimerkiksi kyseeseen, jos rekisteröidytään jollekin keskustelufoorumille, jossa keskustelua seurataan ilman suoraa kontaktia keskustelijoihin. Tarkkailuun ja suunnitelmalliseen tarkkailuun verrattuna kyse olisi kuitenkin nimenomaan pyrkiä henkilökohtaiseen tapaamiseen tai vastaavanlaiseen vuorovaikutukseen kohteen kanssa. Kyse ei kuitenkaan ole pitkäkestoisesta kanssakäymisestä ja luottamussuhteen rakentamisesta, kuten peitetoiminnalle on ominaista. Peitelty tiedonhankinta ei näin ollen ole soluttautumista, eikä menetelmää saa käyttää peitetoimintaa koskevan sääntelyn kiertämiseksi. (HE 203/2017 vp, s. 227.)

Peitelty tiedonhankinta on peitetoimintaa kevyempi menettely, jonka käyttäminen tulee kyseeseen lyhytkestoisissa tilanteissa. Peitetoiminta on kuitenkin tarpeettoman raskas menettely lyhytkestoista tiedonhankintaa varten. Peiteltyyn tiedonhankintaan kuuluu läheisesti myös toiminnan suojaaminen, johon kuuluu väärien, harhauttavien tai peiteltyjen tietojen käyttäminen. HE:n esimerkin mukaan tällä tarkoitetaan esimerkiksi kuljetustoimintaa harjoittavan yrityksen tunnusten käyttäminen harhauttamiseen. (HE 203/2017 vp, s. 228.)

Sotilastiedustelun suojaamisesta säädetään lain 5 luvun 75 §:ssä seuraavasti:

> 75 §

> Sotilastiedustelun suojaaminen
>
> Sotilastiedusteluviranomainen saa käyttää vääriä, harhauttavia tai peiteltyjä tietoja, tehdä ja käyttää vääriä, harhauttavia tai peiteltyjä rekisterimerkintöjä sekä valmistaa ja käyttää vääriä asiakirjoja, kun se on välttämätöntä sotilastiedustelun paljastumisen estämiseksi.
>
> Edellä 1 momentissa tarkoitettu rekisterimerkintä on oikaistava sen jälkeen, kun momentissa tarkoitettuja edellytyksiä ei enää ole. (Laki sotilastiedustelusta, 2019.)

Hallituksen esityksen mukaan tiedustelun suojaamista voidaan tehdä myös tietoverkoissa. Tällainen saattaa tulla kysymykseen esimerkiksi erilaisten palveluiden hankinnan yhteydessä. Suojaamiseen liittyy kuitenkin selkeät perusteet eikä suojaamiseen kovin kevyesti voida ryhtyä. (HE 203/2017 vp, s. 298.)

Samoin poliisilain 5 a luvun 36 §:ssä säädetään siviilitiedustelun suojaamisesta:

> 36 § (26.4.2019/581)
>
> Siviilitiedustelun suojaaminen
>
> Suojelupoliisi saa käyttää vääriä, harhauttavia tai peiteltyjä tietoja, tehdä ja käyttää vääriä, harhauttavia tai peiteltyjä rekisterimerkintöjä sekä valmistaa ja käyttää vääriä asiakirjoja, jos se on välttämätöntä siviilitiedustelun suojaamiseksi. (Poliisilaki, 5 a luku, 2019.)

### 4.5.3 Peitetoiminta ja soluttautuminen

Poliisilain 5 luvun 28 §:ssä säädetään peitetoiminnasta seuraavasti:

> 28 §
>
> Peitetoiminta ja sen edellytykset
>
> Peitetoiminnalla tarkoitetaan tiettyyn henkilöön tai hänen toimintaansa kohdistuvaa suunnitelmallista tiedonhankintaa käyttämällä soluttautumista, jossa tiedonhankinnan edellyttämän luottamuksen hankkimiseksi tai tiedonhankinnan paljastumisen estämiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka valmistetaan tai käytetään vääriä asiakirjoja. (Poliisilaki.)

Peitetoiminnan määrittelystä käy ilmi selkeä ero, joka peitetaktiikoiden välillä on. Peitetoiminnassa on kyse soluttautumisesta kohteen toimintaan, joka on suurin ero verrattuna muihin peite- ja tarkkailutaktiikoihin. Pykälän 3 momentissa on säädetty erikseen peitetoiminnasta tietyin edellytyksin tietoverkoissa seuraavasti:

> Poliisilla on oikeus kohdistaa rikoksen estämiseksi henkilöön peitetoimintaa tietoverkossa, jos henkilön lausumien tai muun käyttäytymisen perusteella voidaan perustellusti olettaa hänen syyllistyvän sellaiseen rikokseen, josta säädetty ankarin rangaistus

> on vähintään kaksi vuotta vankeutta tai jos kysymyksessä on rikoslain 17 luvun 19 §:ssä tarkoitettu rikos. (Poliisilaki.)

Siviilitiedustelussa peitetoimintaa voidaan kohdistaa myös henkilöryhmään, tietojen hankkimiseksi vakavasti kansallista turvallisuutta uhkaavasta toiminnasta. Tämä ilmenee myös poliisilain 5 a luvun 17 §:ssä, jossa säädetään peitetoimintaa koskevasta esityksestä ja suunnitelmasta siviilitiedustelussa.

Soluttautumista olisi mahdollista kohdistaa myös sellaiseen henkilöryhmään, jonka toteuttamasta tai taustalla olevasta toiminnasta olisi tarkoituksena saada tietoja. Kyseessä voi olla esimerkiksi hybridivaikuttaminen, jota ulkomainen tiedustelupalvelu pyrkii suorittamaan. Toiminta itsessään voi olla esimerkiksi pyrkimys ohjata laajamittaista maahantuloa Suomeen. (HE 202/2017 vp, s. 193.) Myös sotilastiedustelussa peitetoimintaa voidaan kohdistaa henkilöryhmään, jossa tarkoituksena ei ole kohdistaa peitetoimintaa kaikkiin ryhmän yksittäisiin henkilöihin. Myös sotilastiedustelua koskevassa lakiesityksessä on mainittu hybridivaikuttaminen eräänä tavoitteena peitetoiminnan osalta. (HE 203/2017 vp, s. 98.)

Päätöksentekoon liittyen yksinomaan tietoverkoissa suoritettavasta peitetoiminnasta voi ns. tavallisesta peitetoiminnasta poiketen päättää myös ”tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies” (Poliisilaki, 5 a luku).

Sotilastiedustelulain 43 §:ssä säädetään peitetoiminnasta, jossa tietoverkoja koskevasta peitetoiminnasta on sanottu:

> Sotilastiedustelun viranomaisilla on oikeus kohdistaa henkilöön tai henkilöryhmään peitetoimintaa tietoverkossa, jos sillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta. (Laki sotilastiedustelusta, 2019.)

HE:n mukaan tietoverkoissa tapahtuvalle ihmisten väliselle vuorovaikutukselle on tyypillistä, että toisen osapuolen henkilöllisyydestä ei ole varmuutta. Tällöin tietoverkkotoiminnassa tulee arvioida, minkälaisia toimia PV:n sotilastiedusteluviranomainen suorittaa. Tietoverkoissa tapahtuvaa peitetoimintaa on myös kuvattu toteuttamisen osalta huomattavasti kevyemmäksi ja turvallisemmaksi verrattuna tavalliseen peitetoimintaan. Tietoverkoissa toteutettavan peitetoiminnan on arvioitu olevan pääasiallisen toimivaltuus koskien peitetoimintaa. (HE 203/2017 vp, s. 255.)

Peitetoiminnassa verkossa tulee huomioida esimerkiksi rekisteröitymistilanteet, joissa palvelu vaatii vahvaa sähköistä tunnistetta, josta taas säädetään vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa. Vahva tunniste vaatii käytännössä peitetoiminnalle tyypillisiä valmistelutoimia ja tietoverkoissa toimiminen tapahtuisi näin ollen ulkoisesti tarkasteltuna vahvaa ulkoista luottamusta herättävän tunnisteen avulla. (HE 203/2017 vp, s. 256.)

Peitetoiminnaksi ei voida katsoa pelkkää rekisteröitymistä avoimelle keskustelufoorumille nimimerkillä ja keskustelun seuraamista, koska peitetoiminta

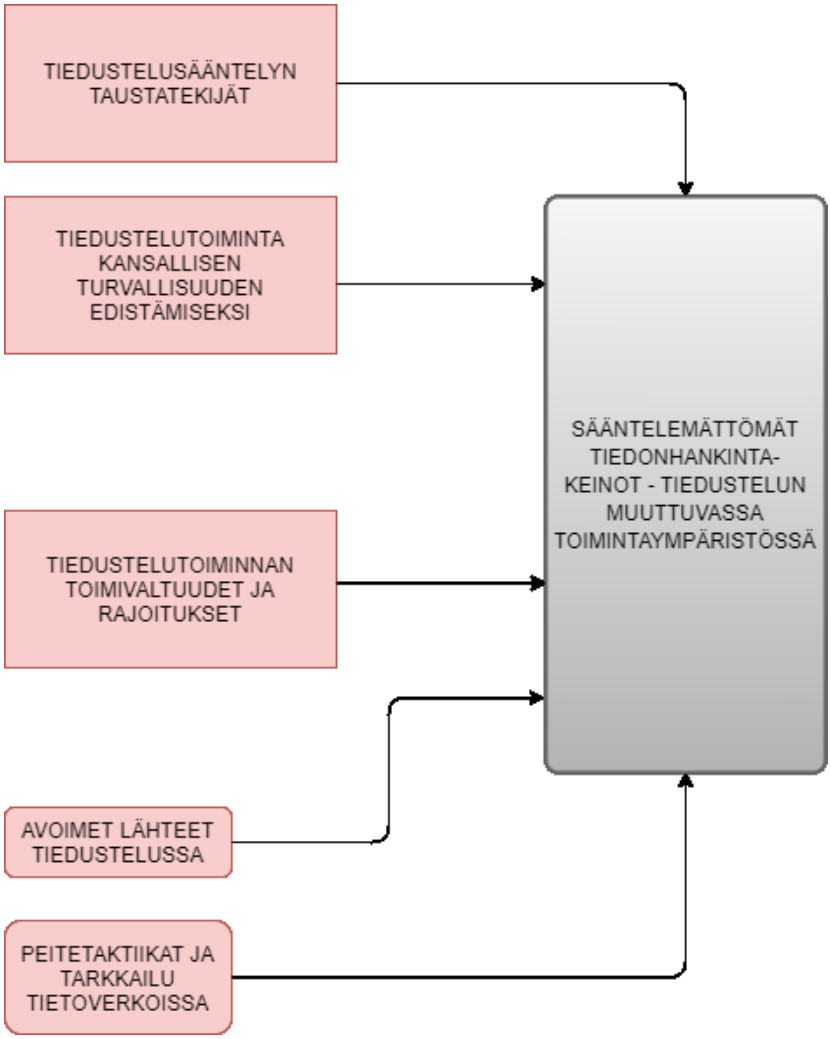
pitää tyypillisesti sisällään luottamuksellisen suhteen saavuttamisen harhauttavien tietojen avulla. Pelkkää rekisteröitymistä tulee pitää peiteltynä tiedonhankintana. (HE 203/2017 vp, s. 256.)

Peitetoiminta myös lasketaan HE 203/2017 vp:n mukaan osaksi henkilötiedustelua (HE 203/2017 vp, s. 90). Tällaisessa tietoverkoissa toteutettavassa peitetoiminnassa voidaankin puhua ns. digitaalisesta henkilötiedustelusta (ks. esimerkiksi Nordström, 2018d, s. 23).

Tietoliikenneverkossa merkittävä osa kapasiteetista käytetään viihdekäyttöön, kuten pelaamiseen tai muuhun lähtökohtaisesti sotilastiedustelun kannalta epärelevanttiin toimintaan. Videoihin liittyvä tiedustelutarve voidaan useimmiten täyttää esimerkiksi peitetoiminnalla tietoverkoissa. (HE 203/2017 vp, s. 277.) Ulkomaan henkilötiedustelua voidaan harjoittaa myös siten, että viestintä tapahtuu Suomesta, mutta tietoverkon viestintäpalveluiden välityksellä (HE 203/2017 vp, s. 221).

# 5 JOHTOPÄÄTÖKSET

Avointen lähteiden tiedustelua suoritetaan tutkimustulosten perusteella joko yksinään tai jonkin toisen tiedonhankintatoimivaltuuden tukena. Tulosten perusteella avointen lähteiden tiedustelun suorittaminen ei myöskään vaadi erillistä sääntelyä tai toimivaltuutta, vaan kyse on ns. normaalista viranomaistoiminnasta. Tiedonhankintakeinoista OSINT:ia vastaa myös tavallinen tarkkailu, jonka suorittaminen ei myöskään tulosten perusteella vaadi erillistä toimivaltuutta. Lisäksi tuloksissa todettiin, että myös esimerkiksi poliisin vihjepuhelin lasketaan tiedonlähteenä sääntelemättömiin tiedonhankintakeinoihin. Tutkimustulokset raportoitiin luokittelussa syntyneiden pääluokkien perusteella, jotka on esitetty alla olevassa kuviossa punaisella. Pääluokkien yhdistäminen tuotti alla esitetyllä tavalla yhdistävän luokan, joka vastaa tämän tutkimuksen tutkimusongelmaan.




KUVIO 6 Analyysin tuloksena syntynyt yhdistävä luokka

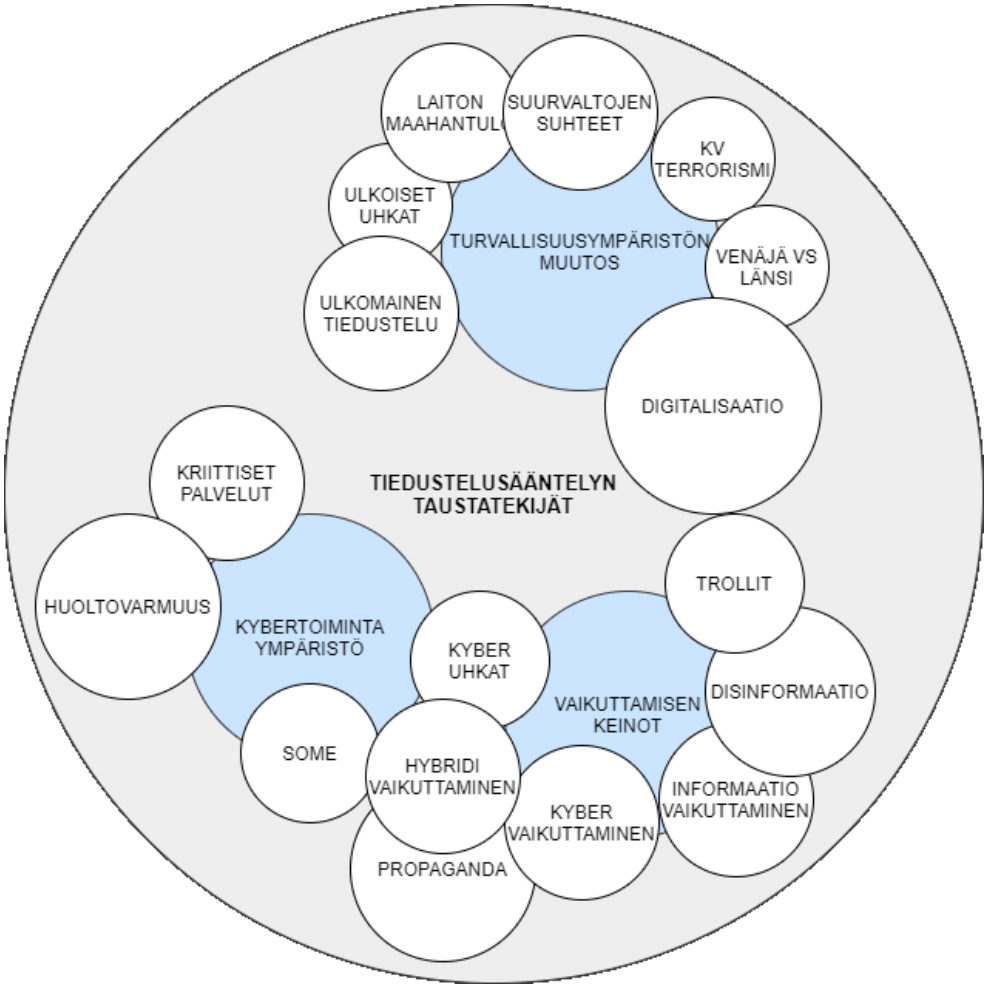
## 5.1 Turvallisuusympäristön muutos

Suomen tiedustelusääntelyn taustalla oli tutkimustulosten mukaan useita tekijöitä ja perusteluita. Lainsäädännöllisesti tiedustelulakien tarkoituksena on taata viranomaisille riittävät toimivaltuudet suorittaa lakisääteisiä tehtäviään ja hankkia tietoa kansallisen turvallisuuden nimissä, laissa säädetyillä toimivaltuuksilla. Konkreettiset perustelut kuitenkin pohjautuvat turvallisuusympäristön muutokseen ja näihin muutoksiin tulee kyetä vastaamaan.

Keskeisiä konkreettisia taustatekijöitä on esitetty alla olevassa kuviossa (kuvio 7), josta käy ilmi, että useat uhkat ja muutokset toimintaympäristössä keskittyvät tietoverkkoihin sekä globalisoitumis- ja digitalisaatiokehitykseen. Kuvio ei ole tyhjentävä, vaan siihen on kerätty eräitä keskeisiä tekijöitä. Tarkastelemalla turvallisuusympäristön muutosta ja siihen liittyviä ilmiöitä, voidaan päätellä kohteita, joihin avointen lähteiden tiedustelua voidaan kohdistaa. Tulosten perusteella avointen lähteiden tiedustelua käytetään ainakin mediaseurantaan, tietyn laajemman ilmiön tai maantieteellisen alueen seurantaan ja tietyn henkilön seurantaan sosiaalisessa mediassa.

Useista tietoverkoissa tapahtuvista ilmiöistä on ainakin periaatteessa mahdollista saada tietoa avointen lähteiden tiedustelulla. Tutkimustulosten perusteella tietoverkoissa käytetään laajasti erilaisia vaikuttamiskeinoja. Esimerkiksi sosiaalisen median rooli on korostunut entisestään ja sieltä on mahdollista saada tietoja useista eri ilmiöistä, tapahtumista ja henkilöistä. Sosiaalisessa mediassa levitetään tulosten perusteella muun ohella disinformaatiota ja propagandaa. Tällaista toimintaa voidaan havaita avointen lähteiden tiedustelulla. Ilmiöiden seuraamisen lisäksi sosiaalisesta mediasta on ainakin joissain tapauksissa mahdollista saada tietoja myös tietystä kohdehenkilöstä. Lisäksi tuloksista käy ilmi, että esimerkiksi terroristit tai muut radikalisoituneet henkilöt saattavat mainostaa suunnitelmistaan sosiaalisessa mediassa tai hakea hyväksyntää toiminnalleen.

Tietoverkoissa tapahtuva vaikuttaminen on turvallisuusympäristön muutoksessa suuressa roolissa tutkimustulosten perusteella. Näin ollen on ainakin teoriassa kannattavaa panostaa myös avointen lähteiden tiedusteluun ja pyrkiä seuraamaan erilaisia ilmiöitä ja tuottamaan ajantasaista tilannetietoa halutusta kohteesta. Resurssit ovat kuitenkin rajalliset ja voi olla, että mahdollisuutena on käyttää myös tehokkaampaa toimivaltuutta tiedon hankkimiseksi, eikä avointen lähteiden tiedusteluun kannata resursseja käyttää. Avointen lähteiden tiedustelutietoa voidaan myös verrata muilla tiedonhankintakeinoilla saatuihin tietoihin ja vahvistaa tietyn tietoverkoissa tapahtuvan ilmiön olemassaoloa. Turvallisuusympäristön muutoksessa keskeinen käsite on myös ns. kybertoimintaympäristö, jonka kannalta on olennaista etsiä tietoa esimerkiksi erilaisista haavoittuvuuksista ja pyrkiä ennalta estämään kyberuhkia. Myös haavoittuvuustietoja voidaan kerätä avointen lähteiden tiedustelulla.




KUVIO 7 Keskeisiä tiedustelusääntelyn taustatekijöitä

## 5.2 Avoimet lähteet ja toimivaltuussääntely

Avointen lähteiden tiedustelu ei vaadi erillistä toimivaltuussääntelyä, sillä siitä ei perustuslain mukaan tarvitsee erikseen lailla säätää. Avointen lähteiden tiedustelu määritellään sellaiseksi tiedonhankinnaksi, jonka ei katsota loukkaavaan yksityisyyden suojaa. OSINT :iin ei kuitenkaan katsota kuuluvan ns. aktiivista osallistumista esimerkiksi tietoverkoissa käytävään keskusteluun tiedon saamiseksi. Avointen lähteiden tiedustelua määritellään myös siten, että siinä kyse on sellaisista tiedoista, joita kuka tahansa voi itse pyytää tai havainnoida. Tietoa voidaan lisäksi hankkia myös ostamalla tai kolmansien osapuolien avulla. Lisäksi myös ns. tavallinen tarkkailu lasketaan OSINT :n kanssa samaan kategoriaan, jossa erillistä toimivaltuussääntelyä ei tarvita. Tutkimustulosten perusteella erityisesti Internetiä koskevan tarkkailun osalta vallitsee käsitys, että erityistä toimivaltuussääntelyä ei tarvita. Tämä määrittely pätee silloin, kun tarkkailua suoritetaan yleisissä tietoverkoissa, esimerkiksi keskustelupalstalla. Tietoverkoissa tapahtuvaa tarkkailua määritellään passiiviseksi tiedonhankinnaksi, jossa tarkkaillaan ihmisten välistä vuorovaikutusta. Lisäksi myös tietyn

muun kohteen, kuten rakennuksen tai tilan tarkkailu ei ole varsinaisen tarkkailutoimivaltuuden käyttöä ja myöskään tällaisesta tiedonhankinnasta ei tarvitse erikseen lailla säätää. Esimerkiksi kiikarin tai kameran käyttö tarkkailussa ei myöskään muuta toimenpiteen luonnetta aistein tehtävään tarkkailuun verrattuna.

EU:n tuomioistuimen mukaan henkilön viestinnästä tai paikkatiedoista kerätyt tiedot pitkällä aikajänteellä muodostavat tietojen kokonaisuuden, jolla voidaan mahdollistaa hyvinkin tarkkojen päätelmien tekemisen niiden henkilöiden osalta, joiden tietoja säilytetään yksityiselämästä, esimerkiksi elämäntavoista, oleskelupaikoista, päivittäisestä tai muusta liikkumisesta ja sosiaalisista suhteista sekä sosiaalisesta ympäristöstä. Yllä mainittujen tietojen pohjalta voidaan laatia henkilön profiili, joka on yksityiselämän kannalta yhtä arkaluontoista, kuin tieto itse viestinnän sisällöstä. Tuomioistuin on pitänyt viestinnän liikenne- ja paikkatietojen säilyttämistä vakavana puuttumisena henkilöiden perusoikeuksiin ja näin ollen vain vakavaksi luokitellun rikollisuuden torjuminen voi olla riittävä peruste tällaiseen toimenpiteeseen.

Mielenkiintoista OSINT:n kannalta on se, että esimerkiksi tietyn henkilön sosiaalisen median tilejä ja muita tekemisiä verkossa seuraamalla voidaan saada hyvinkin tarkka kuvaus siitä, mitä myös yläpuolella on esitetty. Tällöin jouduttaisiin pohtimaan OSINT:n käyttöä aivan uudelta kantilta, sillä perustuslain mukaan avointen lähteiden tiedustelusta ei tarvitse erikseen lailla säätää, koska avointen lähteiden tiedustelun ei katsota loukkaavan yksityisyyden suojaa. Käytännössä jouduttaisiin pohtimaan sitä, voidaanko kaikkia tietoja tosiasiallisesti edes kerätä, koska tarkan ja yksityiskohtaisen profiilin muodostaminen tietystä henkilöstä olisi mahdollista. Toisaalta henkilö on itse omalla toiminnallaan OSINT:n tapauksessa saattanut kyseiset tiedot yleisesti saatavaksi, jolloin aiemmin esitetty OSINT:n määrittely ”tiedot, joita jokainen kansalainen voi itse pyytää tai havainnoida” – täyttyy. Yllä esitetyssä esimerkissä ei kyse myöskään ole aktiivisesta osallistumisesta, jota OSINT:iin ei määritelmän mukaan lasketa. Näin ollen kyse ei myöskään tältä osin ole OSINT:n soveltamisalan ulkopuolelle laskettavasta tiedustelutoiminnasta. OSINT:n tapauksessa myöskään tiedonhankinnan kohteella ei voi olla samanlaista olettamusta yksityisyydestä, kuin esimerkiksi yksityisessä tekstiviestiviestinnässä.

Avointen lähteiden tiedustelutietoja ovat määritelmän mukaan sellaiset tiedot, joita kuka tahansa voi itse pyytää tai havainnoida. Näin ollen tällaisiin tietoihin lasketaan myös esimerkiksi tietovuotojen yhteydessä vuodetut tiedot. Tietovuodoissa kuitenkin asetetaan verkkoon kaikkien nähtäville myös sellaisia tietoja, jotka voivat olla yksityisiä, salaisiksi luokiteltuja tai muuten vain arkaluontoisia. Tämä asetelma aiheuttaa vähintäänkin pohdintaa siitä, onko tällaisten tietojen hyödyntäminen eettistä tai ylipäätään laillista pelkästään OSINT:n keinoin, sillä tilanne voi olla se, että kyseisiin tietoihin käsiksi pääseminen on voinut vaatia tietojen vuotajalta laittomia toimenpiteitä. OSINT:n määritelmä ei kuitenkaan ota kantaa siihen, miten tiedot ovat kaikkien nähtäväksi tulleet, vaan kantaa otetaan vain siihen, miten avoimesti saatavilla olevia tietoja hankitaan – eli havaitsemalla tai pyytämällä. Tässä esimerkissä tietojen hyödyntämistä voidaan

tarkastella myös ”suuremman hyvän” kantilta eli vahinko on jo tapahtunut, mutta tietojen hyödyntämistä voidaan oikeuttaa esimerkiksi sillä, että tietoja käytetään seuraavan rikollisen toiminnan estämiseksi. Lisäksi vain lakia tulkitsemalla tullaan siihen johtopäätökseen, että tässä tapauksessa tiedot ovat julkisesti saatavilla ja kenen tahansa havaittavissa. Tietovuotoja voidaan tiedustelun osalta tulkita myös siten, että tiedustelun kannalta on olennaista tietää, mitä muut tietävät.

Tässä tutkimuksessa käsitelty muutos toimivaltuuksien käyttöön ja uhkaperusteiseen lähestymistapaan liittyen ei kuitenkaan muuta mitään avointen lähteiden tiedustelun osalta, vaan avointen lähteiden tiedustelua on voitu käyttää samalla tavalla myös aiemminkin. Muutos kuitenkin koskee avointen lähteiden tiedustelua siten, että nyt tiedusteluviranomaisilla on käytössään laajasti myös muita menetelmiä, jolloin avointen lähteiden tiedustelun rooli todennäköisesti pienenee suhteessa muihin menetelmiin. Toisaalta avointen lähteiden tiedustelua voidaan suorittaa vapaammin, eikä erityistä säädösperustaa ole, jolloin myös sen käyttäminen on edelleen kevyempää esimerkiksi päätöksenteon osalta.

Olennaista päätöksenteon osalta on se, kuinka OSINT:ia voidaan suorittaa ja kuka sen suorittamisesta päättää. Selvää on se, että tuomioistuimen lupaa edellyttävät tiedustelumenetelmät ovat kaukana OSINT:sta. Niin sanotusti ”kevyin” päätösporras tarkoittaa sitä, että menetelmän käytöstä voi päättää siviilitiedustelussa suojelupoliisin päällystöön kuuluva poliisimies ja sotilastiedustelussa sotilaslakimies tai muu virkamies. Näin ollen OSINT:n sääntelemättömyyden perusteella sen käytöstä voidaan päättää kyseisellä ”kevyimmällä” päätöksentekoportaalla, eikä esimerkiksi raskaampaa tuomioistuinmenettelyä tai suojelupoliisin/pääesikunnan tiedustelupäällikköä vaadita. Laki ei kuitenkaan ota kantaa siihen, kuinka avointen lähteiden tiedustelun suorittamisesta, tai muusta sääntelemättömästä tavallisesta viranomaistoiminnasta päätetään, jolloin toinen tulkita on se, että mitään päätöksentekoa ei vaadita, vaan kyse on enemmänkin siitä, että onko OSINT:sta tai tarkkailusta todellista hyötyä tiedustelutehtävälle.

Viranomaisten toimintaa säädellään yleisesti laissa. Julkisen vallan käytön tulee aina perustua lakiin ja valtionhallinnon toimielinten yleisistä perusteista on säädettävä lailla, jos julkisen vallan käyttö tulee niiden tehtävissä kysymykseen (Rytkölä, 2018, s. 2). Demokraattisessa yhteiskunnassa turvallisuuden takaamiseksi suoritettujen viranomaisten tehtävien on perustuttava lainsäädäntöön (Mickelsson, 2018, s. 1). Perustuslaissa on säädetty seuraavasti: 2 §:n 3 momentin mukaan ”Julkisen vallan käytön tulee perustua lakiin. Kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia” (Suomen perustuslaki, 1999).

Näin ollen kaiken viranomaisen toiminnan tulee perustua lakiin, eikä viranomaisten toiminta käsitä esimerkiksi henkilökohtaisten tietotarpeiden täyttämistä, hyödyntämällä viranomaisten resursseja. Kuten luvussa 4.4 todettiin, avointen lähteiden tiedustelu luetaan ”normaaliin viranomaistoimintaan”, jota rajataan tehtäväsääntelyllä, jolloin toiminnalla tulee olla jokin kytkös kansallisen turvallisuuden suojaamiseen. Avointen lähteiden tiedustelun suorittaminen ei kuitenkaan edellytä sellaisen kohteena olevan toiminnan osoittamista, joka muodostaa vakavan uhkan kansalliselle turvallisuudelle. Avointen lähteiden

tiedustelun käytön välttämättömyyttä ei myöskään tarvitse osoittaa, jolloin luvussa 4.2.2 esitettyä välttämättömyysvaatimusta ei vaadita. Tutkimustulosten perusteella myöskään tuloksellisuusvaatimusta ei OSINT:n kohdalla ole, koska OSINT:n käyttö ei edellytä sellaisen kohteena olevan toiminnan osoittamista, joka muodostaa vakavan uhkan kansalliselle turvallisuudelle.

Tutkimustulosten perusteella myöskään esimerkiksi kuuloetäisyydellä käytävä keskustelu ei nauti luottamuksellisen viestin suojaa, sillä sitä on mahdollista aistein havaita. Näin ollen myös kuka tahansa voi kyseistä keskustelua havainnoida. Rajoitus luottamuksellisen viestin salaisuuden suojaan täyttyy kuitenkin välittömästi silloin, kun luottamukselliseksi tarkoitettua keskustelua kuunnellaan esimerkiksi teknisellä apuvälineellä. Tästä esimerkistä voidaan myös johtaa rajat avointen lähteiden tiedustelulle, kuten myös OSINT:n määritelmässä todetaan: ”—tiedot, joita kuka tahansa voi itse pyytää tai havainnoida”.

Tutkimustuloksissa myös todettiin, että tiedustelutoiminnassa sovelletaan yleisiä periaatteita. Suhteellisuusperiaatteen mukaan haittojen, kuten rajoituksen kohteen yksityisyyden suojaan, tulee olla järkevästi suhteutettuja tavoiteltuun päämäärään nähden. OSINT:ssa ei kuitenkaan puututa yksityisyyden suojaan, joten varsinaista suhteellisuusperiaatteen tarkastelua tuskin joudutaan tekemään. Vähimmän haitan periaatteeseen liittyy läheisesti välttämättömyysvaatimus, jonka mukaan tiedonhankintamenetelmän tulee olla välttämätöntä sekä keinoista tulee valita se, joka vähiten aiheuttaa esimerkiksi puuttumista perusoikeuksiin. Näin ollen myöskään vähimmän haitan periaatteen tarkastelua tuskin OSINT:n kohdalla tarvitsee tehdä. Tarkoitussidonnaisuuden periaatteen mukaan silloin, kun puututaan kohteen oikeuksiin, tulee toimivaltuussäännöksen olla laissa. OSINT:ssa ei puututa perusoikeuksiin, jolloin toimivaltuussääntelyn tarkastelua ei tarvitse tehdä, mutta OSINT:n tulee kuitenkin jollain tavalla kytkeytyä viranomaisen toimintaan, eikä tiedonhankintaa voi tehdä esimerkiksi henkilökohtaisiin tarkoituksiin.

Avointen lähteiden tiedustelussa voidaan ainakin teoriassa löytää myös henkilötietoja, jolloin kyseeseen tulee myös henkilötietojen käsittelyä koskeva lainsäädäntö. Tutkimustulosten perusteella henkilötietojen käsittelyä koskeva sääntely on tiedusteluviranomaisten osalta selkeää. Puolustusvoimille on säädetty oma laki henkilötietojen käsittelystä ja poliisille omansa. Lisäksi sovelletaan lakia henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä. Tiedusteluviranomaisten osalta ei sovelleta yksiselitteisesti mitään muita henkilötietolakeja.

Tiedustelumenetelmien käytöstä tulee tietyissä tapauksissa ilmoittaa tiedustelun kohteelle ja myös tähän sääntelyyn liittyy useita asianhaaroja. Pääsääntönä kuitenkin on, että ilmoittaminen voi tulla ja tulee kysymykseen silloin, kun tiedustelumenetelmien käytöllä puututaan kohteen luottamuksellisen viestin suojaan. Tällöin ilmoittamisvelvoitetta ei avointen lähteiden tiedustelun osalta tarvitse käsitellä, koska avointen lähteiden tiedustelulla ei lähtökohtaisesti kajota kohteen perusoikeuksiin. Tiedustelumenetelmien käytön yhteydessä saatetaan tuottaa myös ns. ylimääräistä tietoa. Pääsääntönä kuitenkin ylimääräisen tiedon osalta on, että:

> Tiedustelumenetelmän käytöllä hankittua tiedustelutehtävään liittymätöntä tietoa saa käyttää toisen käynnissä olevan tai tulevan tiedustelutehtävän suorittamisessa, jos tieto olisi saatu hankkia samalla tiedustelumenetelmällä kuin tiedustelutehtävään liittymätön tietokin hankittiin. (Laki sotilastiedustelusta 88 §, 2019.)

Tällöin OSINT:n keinoin hankitut tiedot eivät kuulu hävittämisvelvollisuuden piiriin ja OSINT:n keinoin hankittuja tietoja voidaan myös käyttää lähtökohtaisesti vapaasti tiedustelutoiminnassa.

## 5.3 Avoimet lähteet toiminnan tukena

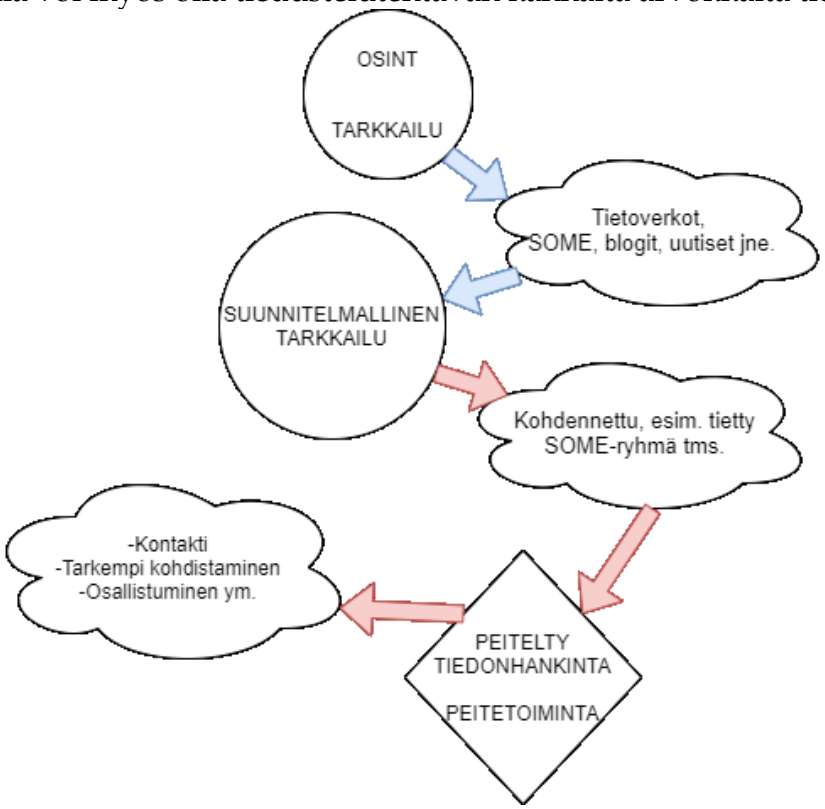
Tyypillisiä tietolähteitä ovat kirjallisuus, kartat, lehdet, tilastot, julkaisut, yleisölle suunnatut televisio- ja radiolähetykset sekä SOME-sisällöt. Tiedonhankinta voidaan OSINT:ssa jakaa joko rajattuun tiedustelukysymykseen perustuvaan tiedonhankintaan tai mediaseurantaan. Lisäksi OSINT:lla tarkoitetaan myös esimerkiksi tiedon hankintaa julkisista tiedotusvälineistä, julkisista viranomaisrekistereistä, julkisista tietokannoista ja julkisuudessa avoimesti esitetyistä lausumista. Internet käsitetään OSINT:ssa omana kanavanaan tiedon hankkimiseksi, eikä niinkään omana tiedonlähteenään.

OSINT:ia käytetään yksinään erityisesti silloin, kun muiden menetelmien käyttö ei ole tehokasta tai mahdollista. Avointen lähteiden osalta tiedostetaan se, että tietoa on saatavilla valtavasti ja väärien tietojen mahdollisuus on suuri. OSINT:n vahvuuksiin kuuluu mm. sen nopeus, maantieteellinen rajoittamattomuus, edullisuus ja mahdollisuus kerätä tietoja myös tulevista tapahtumista. Lisäksi pelkästään OSINT:n keinoin tuotettu tiedustelutuote on tyypillisesti suojaustasoltaan muita tiedustelutuotteita julkisempi, minkä ansioista OSINT-tuotteen käytettävyys on parempi. Tiedonhakua ei kokonaisuudessaan voida tulosten mukaan kuitenkaan perustaa pelkästään avoimiin lähteisiin, sillä tiedustelun tarkoituksena on torjua sellaisia hankkeita, joita valmistellaan salassa. Tuloksissa todettiinkin, että avoimista lähteistä saadut tiedot usein yhdistetään muiden lähteiden tietoihin tilannekuvan muodostamiseksi kansainvälisestä turvallisuusympäristöstä. Pitkäkestoista tiedonhankintaa ja seurantaa kohdistetaan myös esimerkiksi yksittäisiin SOME-tileihin, jota pidetään tärkeänä tietyn tapahtuman ymmärtämiseksi ja tiedon luotettavuuden arvioimiseksi.

Peitetoiminnalla tarkoitetaan tiettyyn henkilöön tai tämän toimintaan kohdistettua suunnitelmallista tiedonhankintaa soluttautumalla ja tiedonhankinta sekä tiedonhankinnan paljastumisen estäminen edellyttävät luottamussuhteen muodostamista. Peitetoiminnassa voidaan näin ollen käyttää vääriä, harhauttavia tai peiteltyjä tietoja sekä rekisterimerkintöjä ja käyttää vääriä asiakirjoja. Peitetoiminnan osalta voidaan pohtia OSINT:n tukea tehtävän suorittamiseksi. Tietoverkoissa toteutettava peitetoiminta on myös arvioitu pääasialliseksi peitetoiminnan toimivaltuudeksi. OSINT:n avulla voidaan päästä käsiksi tietoverkoissa hyödyllisiin tietoihin peitetoiminnan suorittamiseksi. OSINT:ia voitaisiin käyttää

esimerkiksi kohteeseen tutustumiseen ennen tietoverkoissa suoritettavan peitetoiminnan aloittamista.

Alla olevassa kuviossa (kuvio 8) on esitetty tulkinta siitä, kuinka avointen lähteiden tiedustelua tai tarkkailua voitaisiin esimerkiksi käyttää toiminnan ohjaamiseksi ja tukemiseksi. Aluksi kuvion mukaisesti kerättäisiin tietoja sääntelemättömillä tiedonhankintakeinoilla, jonka jälkeen siirryttäisiin käyttämään toimivaltuutta vaativaa suunnitelmallista tarkkailua, joka pohjautuu aiempiin tietoihin. Suunnitelmallisella tarkkailulla taas saataisiin lisää viitteitä siitä, että tiedon hankkimiseksi kansallista turvallisuutta uhkaavasta toiminnasta tulee käyttää tehokkaampaa toimivaltuutta, jolloin voitaisiin siirtyä esimerkiksi peiteltyyn tiedonhankintaan tai peitetoimintaan. Alla oleva päättelyketju voisi tapahtua myös muussa järjestyksessä, eli sääntelemättömien tiedonhankintakeinojen jälkeen siirryttäisiin käyttämään suoraan esimerkiksi peitetoimintaa. Voi tietysti myös olla, että toimivaltuuden käytölle ei jatkossa enää perusteita olekaan, jolloin siirryttäisiin takaisin sääntelemättömiin menetelmiin. Kuvion tarkoituksena on kuitenkin esittää tulkinta siitä, että sääntelemättömät tiedonhankintakeinot voivat toimia tiedustelua tukevina, ohjaavina ja tehostavina menetelminä. Alapuolella esitetystä kuviosta käy myös ilmi toimivaltuussääntelyn erot. Esimerkiksi verrattuna tavalliseen tarkkailuun, suunnitelmallinen tarkkailu vaatii perusteen. Tietoverkoissa tapahtuvassa tarkkailussa saatetaan myös tarvita toisen valtion virkamiehen apua, jolla olisi tehtävän kannalta olennainen osaaminen tai ominaisuus, esimerkiksi kulttuurin tuntemus tai kielitaito. Toisen valtion virkamiehellä voi myös olla tiedustelutehtävän kannalta arvokkaita tietolähteitä.




KUVIO 8 Tulkinta tiedonhankinnan etenemisestä

Tutkimustulosten perusteella tiedustelun suojaamista voidaan suorittaa myös tietoverkoissa, mutta suojaamiseen liittyy kuitenkin selkeät perusteet eikä suojaamiseen kovin kevyesti voida ryhtyä. Suojaaminen saattaisi tulla tietoverkkojen osalta kysymykseen esimerkiksi silloin, kun hankintaan erilaisia palveluita. Suojaaminen usein liitetään läheisesti peiteltyyn tiedonhankintaan tai peitetoimintaan.

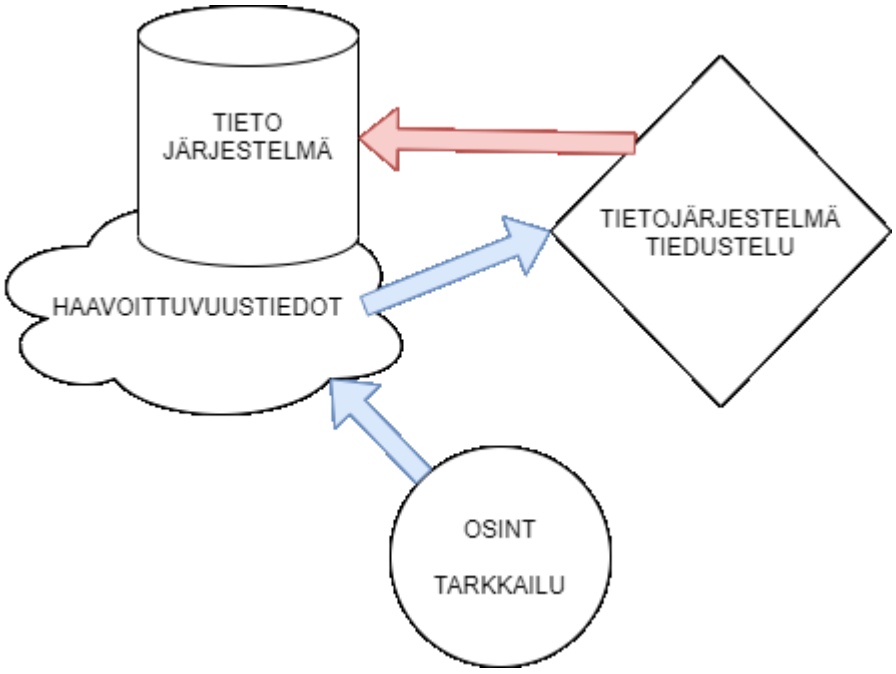
Peitellyssä tiedonhankinnassa pyritään henkilökohtaiseen tapaamiseen tai muuhun vuorovaikutukseen kohteen kanssa. Tämä on myös merkittävä ero tarkkailuun ja suunnitelmalliseen tarkkailuun. Kyse ei kuitenkaan ole peitetoiminnan tavoin soluttautumisesta, jossa tavoitellaan pitkäaikaista luottamussuhdetta kohteen kanssa. Tiedonhankinnan paljastumisen estämiseksi voidaan käyttää pykälän mukaan vääriä, harhauttavia tai peiteltyjä tietoja. Rajanveto peitellyn tiedonhankinnan ja OSINT:n tai tarkkailun välillä tehdään siten, että punnitaan aktiivista osallistumista sekä väärien, harhauttavien ja peiteltyjen tietojen käyttöä. Peitetoiminnaksi ei katsota pelkkää rekisteröitymistä avoimelle keskustelufoorumille nimimerkillä ja keskustelun seuraamista, koska peitetoiminnassa luonteenomaista on luottamussuhteen rakentaminen harhauttavien tietojen avulla. Pelkkää rekisteröitymistä tuleekin pitää peiteltynä tiedonhankintana.

Rekisteröitymistä voidaan tarkemmin pohtia sääntelemättömien keinojen ja peitellyn tiedonhankinnan välillä. Tulkinta on pykälien mukaan se, että peitellystä tiedonhankinnasta voidaan puhua silloin, kun rekisteröitymiseen liittyy harhauttavia, vääriä tai peiteltyjä tietoja. Näin ollen esimerkiksi rekisteröitymistä anonyymina käyttäjänä sosiaalisen median alustalle ilman harhauttavaa vaikutusta, voidaan katsoa myös avointen lähteiden tiedusteluksi tai sääntelemättömäksi tarkkailuksi. Jos kuitenkin palveluun rekisteröityminen vaatii esimerkiksi harhauttavia tai vääriä tietoja, kuten väärän nimen ja henkilöprofiilin käyttämistä, on kyse peitellystä tiedonhankinnasta. Rajanveto näiden välillä ei varmastikaan ole kaikissa tapauksissa täysin selkeä, mutta merkittävin ero lain mukaan tehdään sillä, joudutaanko toiminnassa tekemään esimerkiksi vääriä rekisterimerkintöjä tai asiakirjoja, käyttämään vääriä tietoja ja osallistutaanko vuorovaikutukseen aktiivisesti. Tässä esitetty pohdinta on tulkinta siitä, mitä laissa sanotaan sääntelemättömistä tiedonhankintakeinoista suhteessa säädettyihin toimivaltuuksiin, eikä sitä voida pitää absoluuttisena totuutena, sillä tosiasiassa rajanveto ei välttämättä ole täysin yksiselitteistä. Tässä esitettyä tarkastelua tietoverkkotoiminnan osalta voidaan tiivistää listaamalla tiedonhankintakeinojen pääpiirteet seuraavasti:

1. OSINT/tarkkailu: Ei aktiivista osallistumista, rekisteröityminen esimerkiksi SOME-alustalle nimimerkillä tai muuten käyttämättä vääriä tai harhauttavia tietoja.
2. Peitelty tiedonhankinta: Pyritään lyhytkestoiseen vuorovaikutukseen ja käytetään vääriä, harhauttavia tai peiteltyjä tietoja.
3. Peitetoiminta: Soluttautuminen ja pitkäaikainen luottamussuhde ja käytetään vääriä, harhauttavia tai peiteltyjä tietoja sekä mahdollisesti vääriä rekisterimerkintöjä ja asiakirjoja.

Ulkomaan tietojärjestelmätiedustelulla tarkoitetaan tunkeutumista Suomen rajojen ulkopuolella olevaan tietoverkkoon tai -järjestelmään tietojen hankkimiseksi. Tiedonhankinta tapahtuu tietoteknisiä menetelmiä käyttämällä. Menetelmässä ei kuitenkaan ole kyse hyökkäyksellisestä toiminnasta, vaan kyse on järjestelmän sisältämien tietojen hankinnasta. Mielenkiintoista OSINT:n kannalta on se, että OSINT:ia voidaan mahdollisesti käyttää myös tietojärjestelmätiedustelun maalittamisen tukena. OSINT:n avulla voidaan mahdollisesti löytää esimerkiksi järjestelmään liittyviä haavoittuvuuksia tai muita tietoja, joiden avulla varsinaista toimivaltuutta voidaan käyttää.

Alla olevassa kuviossa (kuvio 9) on esitetty teoreettisen tason tulkinta siitä, kuinka avointen lähteiden tiedustelua tai tarkkailua voitaisiin hyödyntää tiedustelutoiminnan tukena tai tehostajana. Kuviossa on esitetty hypoteettinen tiedonhankinnan eteneminen, jossa OSINT:n tai tarkkailun keinoin hankitaan haavoittuvuustietoja kohteena olevasta tietojärjestelmästä. Näitä tietoja voitaisiin käyttää pohjana tai apuna, jotta varsinaista säädettyä toimivaltuutta voitaisiin kohdejärjestelmään kohdistaa.




KUVIO 9 Toinen tulkinta tiedonhankinnan etenemisestä

Tutkimuksessa huomattiin myös, että avointen lähteiden tiedustelua voidaan käyttää myös tietoliikennetiedustelun tukena, vaikka tietoliikennetiedustelua ei tässä tutkimuksessa käsitelläkään. Tietoliikennetiedustelussa teknisten tietojen käsittelyllä pyritään rajaamaan pois epärelevantti tietoliikenne jo heti tiedustelun alkuvaiheessa. Viestinnän teknisten tietojen avulla pyritään selvittämään, missä viestintäverkon osassa tietyn toimijan tai tietyn maantieteellisen alueen tietoliikenne kulkee. Tässä käsittelyvaiheessa julkisista lähteistä voidaan hankkia tietoa mm. BGP-reitityksestä, joka kertoo autonomisten järjestelmien omistajat, joiden kautta viestintä on tiettyyn pisteeseen kulkenut. Kyseisten järjestelmien omistajat

ovat mm. operaattoreita, jotka vastaavat tietyn IP-osoitealueen reitittämiskokonaisuudesta. Lisäksi tutkimustuloksissa todettiin, että mm. seuraavat julkiset tiedot ja niiden kerääminen tulee olla tiedustelutoiminnassa sallittua:

- Kohde- ja lähdeosoitteet sekä käytetyt protokollat
- Otsikkotiedot yleensäkin
- Liikennemäärät ja nimipalvelukyselyt
- Salaamattoman tietoliikenteen sisältö, kuten salaamaton selainliikenne
- Salaamattomat puhelut, videoneuvottelut sekä sähköpostit
- Palvelinten ja aktiivi- sekä päätelaitteiden haavoittuvuuksien havaitseminen ja haavoittuvuuksien tunnistetietojen kerääminen

Ennen tiedustelulainsäädäntöä tiedonhankinnan kohteena oleva henkilö on pitänyt kyetä yksilöimään vähintäänkin henkilön roolin tai tehtävän perusteella. Näin on ollut myös tilanteessa, jossa kohde on ollut henkilöllisyydeltään ennestään tuntematon. Telekuuntelua ja televalvontaa on voitu kohdistaa tuntemattomaan henkilöön, mutta perusteena on täytynyt esittää esimerkiksi IP-osoite tai IMEI-koodi. Ilman tällaista rikostorjunnallista perustetta salaisia tiedonhankintakeinoja ei ole ollut mahdollista käyttää. Tällöin tiedustelu on ollut vahvasti avointen lähteiden, poliisin yleisvalvonnan ja yhteistyötoiminnan varassa. Avoimia lähteitä on käytetty laajasti ennen tiedustelulainsäädäntöä. Tällöin avointen lähteiden tiedustelusta on myös laaja kokemuspohja ja siinä käytettävät tekniikat ovat tämän perusteella laajasti tiedossa. Avointen lähteiden tietojen käyttö tiedustelua ohjaavana, täydentävänä ja tehostavana menetelmänä on todennäköisesti entistä suuremmassa roolissa, sillä tiedustelulainsäädäntö tarjoaa useita uusia toimivaltuuksia aiempaan verrattuna, eikä tiedustelussa tarvitse nojata avoimiin lähteisiin niin voimakkaasti. Myös tarkkailutyyppisten keinojen avulla voidaan tutkimustulosten perusteella tehostaa tiedustelun vaikuttavuutta. Näillä keinoilla saaduilla reaaliaikaisilla tiedoilla voidaan parantaa merkittävästi tilannekuvaa sekä helpottaa päätöksentekoa tiedustelun suuntaamiseen ja painopisteisiin liittyen. Näin ollen myös Internetissä suoritettavalla sääntelemättömällä tarkkailulla on tunnistettuja hyötyjä.

Tiedustelussa kyky yhdistellä eri lähteiden tietoja on oleellista, eikä kyseessä ole vain salaisilla tiedonhankintakeinoilla hankitut tiedot, vaan myös julkisia lähteitä tulee kyetä hyödyntämään. Kerätty tietokokonaisuus voi olla, ja usein varmasti onkin, monista lähteistä kerätyn tiedon yhdistelmä, jossa yhdistetään avointen lähteiden tietoja muiden menetelmien tuottamiin tietoihin. Tällöin avointen lähteiden tiedot voivat esimerkiksi merkittävästi täydentää tai vahvistaa muita tietoja.

# 6 POHDINTA

Tutkimukselle asetti haasteita se, että avointen lähteiden tiedustelua ei ole merkittävästi tästä näkökulmasta aiemmin tutkittu. Tutkimuksen alussa käsiteltiin aiempia tutkimuksia ja julkaisuja, joissa todettiin, että lainsäädännölliset epävarmuudet ympäröivät avointen lähteiden tiedustelua ja oikeuskäytännöissä on puutteita. Ainakin tiedusteluviranomaisten osalta Suomessa kuitenkin avointen lähteiden tiedustelua koskeva oikeuskäytäntö on tämän tutkimuksen perusteella pääsääntöisesti selkeä. Joitain lainsäädännöllisiä epävarmuuksia OSINT:iin toki liittyy, mutta epävarmuuksia liittyy todennäköisesti myös moniin muihin tiedonhankintakeinoihin. Tarve tiedustelulainsäädännön jatkuvalle tarkastelulla on selkeä, koska toimintaympäristö on muutoksessa ja oikeuskäytäntö jää herkästi jälkeen muuttuvan turvallisuusympäristön vuoksi. Näin ollen tässä tutkimuksessa tutkittiin ajankohtaan nähden ajankohtaista ja tarpeellista aihealuetta. Avointen lähteiden tiedustelua, tietoverkkotoimintaa ja sääntelemätöntä tarkkailua käsitellään lainsäädännössä hyvin niukasti.

Tutkimuksen alussa määriteltiin käsitteitä, jonka mukaan avointen lähteiden tiedustelua on määritelty aiemmissa julkaisuissa ja tutkimuksissa Suomen lainsäädäntöä tarkemmin. Esimerkiksi lähteiden osalta tiedustelulakipaketissa ei otettu lainkaan kantaa ns. harmaisiin lähteisiin. Sosiaalisen median roolia on kyllä lain valmisteluissa korostettu, mutta varsinaisesta sosiaalisen median tiedustelusta lain esitöissä ei puhuta. Muuttuva toimintaympäristö on laajasti huomioitu tiedustelulakipaketin esitöissä, samoin myös aiemmissa julkaisuissa. Avointen lähteiden tiedustelussa käytettäviä tekniikoita ja menetelmiä ei ole käsitelty juuri lainkaan tiedustelulakien esitöissä, mutta aiemmissa julkaisuissa ja tutkimuksissa pääpaino on ollut tekniikoiden käsittelyssä. Mielenkiintoisia osa-alueita, kuten Dark- ja Deepwebiä ei ole lain esitöissä noteerattu lainkaan, eikä myöskään esimerkiksi eroja manuaalisen tietojenkeräyksen ja skriptattujen keräystekniikoiden välillä. Aiemmissa julkaisuissa on todettu, että keräysmenetelmillä voi olla paljonkin merkitystä esimerkiksi oikeudenkäyntejä ajatellen, mutta lain esitöissä tätä aihetta ei ole käsitelty. Väärän informaation ja informaation suuren määrän mahdollisuus on huomioitu lain esitöissä. Tämä näkökulma on laajasti noteerattu myös aiemmissa julkaisuissa. Tiedonkeräysprosessiin liittyviä salaisia komponentteja, kuten tiedonkerääjän henkilöllisyyttä ei ole juuri lain esitöissä käsitelty, mutta aiempien julkaisujen perusteella se on myös olennainen osa-alue OSINT:n suorittamisessa. Todennäköisesti kyse on siitä, että teknisiä yksityiskohtia ei lähtökohtaisesti haluta julkisissa asiakirjoissa tuoda voimakkaasti esille.

Tiedustelutoiminnan kokonaisuus on laaja ja tässä tutkimuksessa pyrittiin etsimään vastauksia siitä yhteen osa-alueeseen. Avointen lähteiden tiedustelua ja sen sääntelemättömyyttä ei kuitenkaan ole mielekästä todeta ilman vertailua säädettyihin toimivaltuuksiin, jolloin päästään käsiksi avointen lähteiden tiedustelun syvällisempään merkityssisältöön. Tällä menettelyllä myös tässä tutkimuksessa saatiin tutkimukselle laajuutta ja kosketuspintaa myös laajemmin

tiedustelutoimintaan. Tiedustelulakien esitöissä puhuttiin kokonaisuudessaan avointen lähteiden tiedustelusta hyvin vähän, samoin kuin myös muista sääntelemättömistä tiedonhankintakeinoista. Tätä selittää osaltaan se, että lakien tarkoituksena oli tuoda viranomaisille uusia toimivaltuuksia ja toimivaltuuksien tarkastelussa täytyi merkittävästi keskittyä mm. perus- ja ihmisoikeuksiin. Toinen johtopäätös on se, että sääntelemättömiä tiedonhankintakeinoja ei ole ollut tarvetta enempää käsitellä, koska niiden käyttö ja luonne katsotaan tiedustelutoiminnassa selkeäksi. Haasteita sääntelemättömien tiedonhankintakeinojen tarkastelulle asettaa kuitenkin se, että toimintaympäristö on muutoksessa ja tietoverkkojen rooli on korostunut. Tietoverkoista on mahdollista ainakin teoriassa saada myös sellaisia tietoja, joiden hankkimiseksi vaadittaisiin säädettyä toimivaltuutta. Tällaiset tilanteet aiheuttavat ainakin pohdintaa avointen lähteiden tiedustelun luonteesta ja käytöstä. Avointen lähteiden tiedustelua koskeva määrittely lainsäädännön osalta myös täsmää suurimmilta osin tuloksissa mainittujen verrokkimaiden määrittelyä julkisista lähteistä ja niiden käytöstä tiedustelutoiminnassa.

## 6.1 Tutkimuksen luotettavuus

Laadullisten tutkimusten yhteydessä esiintyy pohdinta siitä, että tutkimuksen validiutta ja reliaabeliutta on vaikea määritellä, koska tutkittavat ilmiöt, henkilöt ja ympäristöt ovat ainutlaatuisia. Tähän liittyy läheisesti myös se, että ihmiset tulkitsevat ja kokevat asioita eri tavoilla. Laadullisissa tutkimuksissa tutkimuksen luotettavuutta voidaan kuitenkin edistää myös sillä, että tutkija kertoo tarkasti siitä, kuinka tutkimus on toteutettu (Hirsjärvi ym., 2004, s. 216). Tämän tutkimuksen toteutus on yksinkertainen ja selkeä, joka mahdollistaa lukijalle sen, että tutkimusta on helppo seurata. Tämä myös edistää tutkimuksen luotettavuutta. Reliaabeliutta voidaan määritellä siten, että eri tutkimuskerrat tuottavat saman tuloksen tai siten, että kaksi analyytikkoa päätyy samanlaiseen analyysiin (Hirsjärvi & Hurme, 2001, s. 186). Reliaabeliutta voidaan myös määritellä siten, että eri tutkimusmenetelmillä saadaan samoja tuloksia (Hirsjärvi & Hurme, 2001, s. 186). Tämän tutkimuksen päätelmät perustuvat tiedustelulakeihin ja niiden esitöihin, joten tutkimusaineistoa voidaan pitää luotettavana ja kattavana. Lakien tulkinnassa kuitenkin on mahdollista, että eri tutkija voi tulkita samaa lainsäädäntöä eri tavalla. Kuten myös Hirsjärvi ja Hurme toteavat, on kuitenkin epätodennäköistä, että kahdella menetelmällä saadaan tismalleen sama tulos, sillä ihmiset tulkitsevat asioita eri tavoin eri ympäristöissä (Hirsjärvi & Hurme, 2001, s. 186).

Tuomen ja Sarajärven (2018) mukaan kaikille tutkimuksen toteutukseen liittyville analyysitekniikoille ei tarvitse olla nimeä, vaan tutkimuksen toteutuksen tarkka kuvaaminen saattaa riittää luomaan uskottavan tutkimuksen. Heidän mukaansa olennaisempaa on pohtia, miten tutkimuksen analyysin toteuttaa, kuin se miten se nimetään (Tuomi & Sarajärvi, 2018, s. 141). Kvalitatiivisen tutkimuksen luotettavuutta voidaan arvioida Tuomen ja Sarajärven (2018) mukaan myös

johdonmukaisuuden perusteella. Tällä tarkoitetaan sitä, että tutkimuksen komponentit, kuten tutkimuksen kohde ja tarkoitus, tutkijan sitoumukset, aineiston keruu, tutkimuksen kesto, aineiston analyysi ja tutkimuksen raportointi ovat johdonmukaisesti kytköksissä toisiinsa. (Tuomi & Sarajärvi, 2018, s. 122.)

Tämän tutkimuksen aineiston keruu ja analysointi toteutettiin manuaalisena käsityönä, jolloin inhimillisen virheen mahdollisuus on olemassa. Tutkimus kuitenkin koski sitä, mitä sen haluttiinkin koskevan, eli tutkimuksessa selvitettiin, mitä tiedustelulainsäädännössä ja sen esitöissä sanotaan avointen lähteiden tiedustelusta ja sen tukevasta roolista osana tiedustelutoimintaa. Tutkimuksen eteneminen perustui johdonmukaiseen sisällönanalyysiin, jossa tutkimusaineisto jaoteltiin järkevään ja informatiiviseen muotoon. Tässä tutkimuksessa tuotettiin kattava sisällönanalyysi tiedustelulainsäädännön ja avointen lähteiden tiedustelun suhteesta, josta myös ilmenee selkeät erot säänneltyjen ja sääntelemättömien tiedonhankintakeinojen välillä.

## 6.2 Jatkotutkimustarpeet

Avointen lähteiden tiedustelua suoritetaan laajasti myös muissa, kuin tiedustelun toimintaympäristöissä, joten tietyn muun toimintaympäristön tarkastelu vaatii oman tutkimuksensa. Esimerkiksi muiden viranomaisten osalta avointen lähteiden tiedustelua tulisi mahdollisesti tarkastella myös muiden lakien osalta. Näin olisi mahdollista myös saada käsitystä siitä, mihin tarkoitukseen avointen lähteiden tiedustelua muissa toimintaympäristöissä käytetään. Tällä tarkastelulla voitaisiin saada myös käsitystä siitä, millaisia tietoja muissa toimintaympäristöissä avointen lähteiden tiedustelussa käsitellään. Tätä tarkastelua voitaisiin sitten esimerkiksi verrata toiminnassa sovellettavaan lainsäädäntöön. Tutkimuksessa käsiteltävän lain tulkinnan parantamiseksi voitaisiin käyttää myös haastatteluja, jotka tarjoaisivat ensikäden tietoa siitä, kuinka esimerkiksi avointen lähteiden tiedustelua tulkitaan käytännössä suhteessa muuhun toimivaltuussääntelyyn.

# TUTKIMUSAINEISTO

Aapio, L. 2018. HaV 27.02.2018 poliisipäällikkö, poliisikomentaja Lasse Aapio, Helsingin poliisilaitos Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-172951.pdf

Eduskunta. Yleistä oikeuslähteistä ja oikeudellisesta informaatiosta. Haettu 4.9.2020 osoitteesta https://www.eduskunta.fi/FI/naineduskuntatoimii/kirjasto/aineistot/kotimainen_oikeus/kotimaiset-oikeuslahteet/Sivut/Yleista-oikeuslahteista-ja-oikeudellisesta-informaatiosta.aspx

Eduskunta. (2020). Asian käsittelytiedot HE 203/2017 vp. Haettu 4.9.2020 osoitteesta https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_203+2017.aspx

Eduskunta. (2020). Asian käsittelytiedot HE 202/2017 vp. Haettu 4.9.2020 osoitteesta https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_202+2017.aspx

Eronen, P. 2018. PuV 06.04.2018 valmiuspäällikkö Pasi Eronen, Teknologiateollisuus ry Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-180978.pdf

Eränen, M. 2018. LaV 28.02.2018 Poliisihallitus Asiantuntijalausunto haettu 16.9.2020 osoitteesta https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-173137.pdf

Fjäder, C. 2018. HaV 06.03.2018 Johtaja, suunnittelu- ja analyysiosasto Christian Fjäder, Huoltovarmuuskeskus Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-174875.pdf

Fredman, M. 2018. PeV 19.10.2018 oikeustieteen tohtori Markku Fredman Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-216441.pdf

Hakonen, K. 2018b. LaV 02.03.2018 apulaisoikeuskanslerin sijainen Kimmo Hakonen, oikeuskanslerinvirasto Asiantuntijalausunto

https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-174547.pdf

Hallituksen esitys eduskunnalle laiksi sotilastiedustelusta sekä eräiksi siihen liittyviksi laeiksi. HE 203/2017. Haettu osoitteesta https://www.finlex.fi/fi/esitykset/he/2017/20170203

HaVM 36/2018 vp. https://www.eduskunta.fi/FI/vaski/Mietinto/Documents/HaVM_36+2018.pdf

HE 202/2017 vp https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_202+2017.pdf

HE 203/2017 vp https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_203+2017.pdf

Heikkola, H. 2018. PuV 07.03.2018 neuvotteleva virkamies Heli Heikkola, sisäministeriö Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-175281.pdf

Jantunen, S. 2018. HaV 13.03.2018 sotatieteiden tohtori, tutkija Saara Jantunen, Puolustusvoimien tutkimuslaitos Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-176492.pdf

Kaila, U. 2018a. LiV 21.03.2018 tietoturvapäällikkö Urpo Kaila, CSC - Tieteen tietotekniikan keskus Oy Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-179043.pdf

Kaila, U. 2018b. PuV 10.04.2018 tietoturvapäällikkö Urpo Kaila, CSC - Tieteen tietotekniikan keskus Oy Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-181583.pdf

Kolehmainen, S. 2018. HaV 27.02.2018 poliisiylijohtaja Seppo Kolehmainen, Poliisihallitus Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-173013.pdf

Laitinen, K. 2018a. PeV 15.02.2018 poliisiosaston lainsäädäntöjohtaja Katriina Laitinen, sisäministeriö Asiantuntijalausunto

https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-170384.pdf

Laitinen, K. 2018b. PeV 18.10.2018 poliisiosaston lainsäädäntöjohtaja Katriina Laitinen, sisäministeriö Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-215945.pdf

Laki puolustusvoimista. 11.5.2007/551. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2007/20070551?search%5Btype%5D=pika&search%5Bpika%5D=laki%20puolustusvoimista

Laki sotilastiedustelusta. 26.4.2019/590. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2019/20190590?search%5Btype%5D=pika&search%5Bpika%5D=tiedustelu#L4P23

Lavapuro, J. 2018. PeV 23.10.2018 professori Juha Lavapuro Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-218188.pdf

Lehto, M. 2018. LiV 10.04.2018 professori Martti Lehto, Jyväskylän yliopisto Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-181569.pdf

Limnell, J. 2018. UaV 11.04.2018 kyberturvallisuuden professori Jarno Limnéll, Aalto-yliopisto Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-181486.pdf

Melaluoto, J. 2018. UaV 10.04.2018 sotilaslakimies Juho Melaluoto, Pääesikunta Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-181612.pdf

Melander, S. 2018a. LaV 13.03.2018 professori Sakari Melander Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-176221.pdf

Melander, S. 2018b. PeV 18.10.2018 professori Sakari Melander Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-215691.pdf

Meriniemi, M. 2018a. LiV 20.02.2018 lainsäädäntöneuvos Marko Meriniemi, sisäministeriö Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-171455.pdf

Meriniemi, M. 2018b. TrV 13.03.2018 lainsäädäntöneuvos Marko Meriniemi, sisäministeriö Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-177916.pdf

Meriniemi, M. 2018c. PuV 27.9.2018 lainsäädäntöneuvos Marko Meriniemi, sisäministeriö Asiantuntijalausunto A https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-219270.pdf

Meriniemi, M. 2018d. HaV 09.11.2018 lainsäädäntöneuvos Marko Meriniemi, sisäministeriö Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-220936.pdf

Meriniemi, M. 2018e. LaV 28.11.2018 lainsäädäntöneuvos Marko Meriniemi, sisäministeriö Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-226710.pdf

Meriniemi, M. 2018f. HaV 04.12.2018 lainsäädäntöneuvos Marko Meriniemi, sisäministeriö Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-228500.pdf

Meriniemi, M. 2018g. LaV 14.12.2018 lainsäädäntöneuvos Marko Meriniemi, sisäministeriö Asiantuntijalausunto Liite 2 https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-232159.pdf

Mickelsson, M. 2018. PuV 10.04.2018 tietoyhteiskuntasuhdejohtaja Max Mickelsson, Microsoft Oy Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-181602.pdf

Mielonen, T. 2018. UaV 05.04.2018 puheenjohtaja Timo Mielonen, Suomen Sadankomitea ry Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-180742.pdf

Mutanen, A. 2018a. LiV 20.02.2018 erityisasiantuntija Anu Mutanen, oikeusministeriö Asiantuntijalausunto

https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-171458.pdf

Mutanen, A. 2018b. PeV 16.10.2018 erityisasiantuntija Anu Mutanen, oikeusministeriö Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-214101.pdf

Mutanen, A. 2018c. PeV 19.10.2018 erityisasiantuntija Anu Mutanen, oikeusministeriö Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-216439.pdf

Mykkänen, K. 2018. PuV 07.03.2018, sisäministeriö Asiantuntijalausunto haettu 16.9.2020 osoitteesta https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-175103.pdf

Nordström, H. 2018a. PeV 14.02.2018 lainsäädäntöjohtaja Hanna Nordström, puolustusministeriö Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-170140.pdf

Nordström, H. 2018b. LiV 20.02.2018 lainsäädäntöjohtaja Hanna Nordström, puolustusministeriö Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-171449.pdf

Nordström, H. 2018c. UaV 03.04.2018 lainsäädäntöjohtaja Hanna Nordström, puolustusministeriö Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-179885.pdf

Nordström, H. 2018d. LaV 28.11.2018 lainsäädäntöjohtaja Hanna Nordström, puolustusministeriö Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-227090.pdf

Nordström, H. 2018e. LaV 14.12.2018 lainsäädäntöjohtaja Hanna Nordström, puolustusministeriö Asiantuntijalausunto Liite 2 https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-232161.pdf

Ojanen, T. 2018. PeV 25.10.2018 professori Tuomas Ojanen Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-217856.pdf

Pelttari, A. 2018a. HaV 01.03.2018 päällikkö, poliisineuvos Antti Pelttari, suojelupoliisi Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-173472.pdf

Pelttari, A. 2018b. PuV 27.02.2018 päällikkö, poliisineuvos Antti Pelttari, suojelupoliisi Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-172882.pdf

Pohjolainen, T. 2018. PeV 25.10.2018 professori (emeritus) Teuvo Pohjolainen Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-217490.pdf

Poliisilaki 26.4.2019/581. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2011/20110872?search%5Btype%5D=pika&search%5Bpika%5D=tiedustelu#L5aP2

Poliisilaki, 5 a luku. 26.4.2019/581. Haettu 4.10.2020 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2011/20110872#L5a

Puistola, J-A. 2018. HaV 09.03.2018 vanhempi osastoesiupseeri Juha-Antero Puistola, Turvallisuuskomitea Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-175813.pdf

PuVL 16/2018 vp. https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/PuVL_16+2018.pdf

PuVM 9/2018. https://www.eduskunta.fi/FI/vaski/Mietinto/Documents/PuVM_9+2018.pdf

Rytkölä, A. 2018. PuV 13.04.2018 hallituksen puheenjohtaja Antero Rytkölä, Suomen Lakimiesliitto ry Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-182624.pdf

Rönkä, M. 2018. LiV 20.02.2018 ylitarkastaja Maija Rönkä, liikenne- ja viestintäministeriö Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-171402.pdf

Saarelainen, M. 2018. 06.03.2018 johtaja Matti Saarelainen, Euroopan hybridiuhkien torjunnan osaamiskeskus Asiantuntijalausunto

https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-174892.pdf

Scheinin, M. 2018. UaV 09.05.2018 professori Martin Scheinin Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-189042.pdf

Suomen perustuslaki. 11.6.1999/731. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1999/19990731#L2P12

Tammikko, T. 2018. HaV 08.03.2018 vanhempi tutkija Teemu Tammikko, Ulkopoliittinen instituutti Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-175310.pdf

Tiilikainen, T. 2018. HaV 06.03.2018 johtaja Teija Tiilikainen, Ulkopoliittinen instituutti Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-175032.pdf

Vainio, N. 2018. PeV 17.10.2018 oikeustieteen maisteri Niklas Vainio Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-215027.pdf

Vallinheimo, K. 2018. PuV 28.02.2018 budjettineuvos Kirsti Vallinheimo, valtiovarainministeriö Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-173237.pdf

Viljanen, V-P. 2018. PeV 06.11.2018 professori Veli-Pekka Viljanen Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-219722.pdf

Ylitalo, J. 2018. HaV 25.10.2018 valtioneuvoston turvallisuusjohtaja Jari Ylitalo, valtioneuvoston kanslia Asiantuntijalausunto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-217847.pdf

# LÄHTEET


Akhgar, B., Bayerl, P. & Sampson, F. (2016). Open Source Intelligence Investigation: From Strategy to Implementation. Switzerland: Springer International Publishing.

Bazzell, M. (2019). Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. Seventh Edition. Library of Congress Cataloging-in-Publication Data: Application submitted.

Bellingcat's Online Investigation Toolkit. (2020). Bellingcat. Haettu 9.3.2020 osoitteesta https://docs.google.com/document/d/1BfLPJpRtyq4RFtHJoNpvWQjmGnyVkfE2HYoICKOGguA/preview#

Casanovas, P. 2014. Open Source Intelligence, Open Social Intelligence and Privacy by Design. European Conference on Social Intelligence. Haettu 14.4.2020 osoitteesta http://ceur-ws.org/Vol-1283/

Gibson, S. (2011). Open source intelligence (OSINT): a contemporary intelligence lifeline. Cranfield University. PhD, EngD, MPhil and MSc by research theses - CDS – Shrivenham. PhD THESIS. Haettu 4.3.2020 osoitteesta https://dspace.lib.cranfield.ac.uk/bitstream/handle/1826/6524/PHD%20-%20Gibson%2c%20S.pdf?sequence=1&isAllowed=y

Gruszczak, A. (2016). Intelligence Security in the European Union: Building a Strategic Intelligence Community. London: Macmillan Publishers Ltd.

Helenius, M. (2020). Pro gradu -tutkielma. "Tämä ei voi olla kansallisen kokonaisedun mukaista." Suojelupoliisin tiedustelulakeihin liittyvät näkemykset ja perustelut eduskunnan valiokunnille vuoden 2018 valmistelutyön aikana. Helsingin Yliopisto: Valtiotieteellinen tiedekunta. Katsottu 4.9.2020 osoitteesta https://helda.helsinki.fi/bitstream/handle/10138/314357/Helenius_Mikko_Pro_gradu_2020.pdf?sequence=3&isAllowed=y

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

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2004). Tutki ja kirjoita. (10. osin uud. painos). Jyväskylä: Gummerus Kirjapaino Oy.

James Madison University. 2020. Program Overview. Haettu 14.4.2020 osoitteesta https://www.jmu.edu/ia/program/overview.shtml

Johnson, M. (2013). Cyber Crime, Security and Digital Intelligence. Farnham, Surrey : Gower Pub. Ltd.

Juutilainen, K. (2008). Julkisiin lähteisiin perustuva tiedustelu (Open Source Intelligence – OSINT) sotilastiedustelussa. Helsingin Yliopisto: Valtiotieteellinen tiedekunta, Kansainvälinen politiikka. Haettu 5.9.2020 osoitteesta https://helda.helsinki.fi/handle/10138/11034

Kari, M. J. (2019). Luento, Informaation hallinta ja tiedustelu I kurssilla Jyväskylän yliopistolla 9.9.2019.

Kurttila, M. (2015). Pro gradu -tutkielma. Mitä tiedustelusta kirjoitettiin? - Suojelupoliisi ja tiedonhankintalakityöryhmä mediassa 2013-2015. Tampereen Yliopisto: Hallintotiede. Katsottu 4.9.2020 osoitteesta https://trepo.tuni.fi/bitstream/handle/10024/97568/GRADU-1435556231.pdf?sequence=1&isAllowed=y

Lammi, M. (2017). Diplomityö: YEK 58 Ilmasotalinja. Maanpuolustuskorkeakoulu. Haettu 5.9.2020 osoitteesta https://www.doria.fi/bitstream/handle/10024/144305/YEK58_LammiM.pdf?sequence=1&isAllowed=y

Liaropoulos, A. (2013). The Challenges of Social Media for the Intelligence Community. Journal of Mediterranean and Balkan Intelligence, vol.1 no.1 (2013). Haettu 3.3.2020 osoitteesta https://www.academia.edu/3800630/The_Challenges_of_Social_Media_Intelligence_for_the_Intelligence_Community_Journal_of_Mediterranean_and_Balkan_Intelligence_vol.1_no.1_2013_

Lohse, M. & Viitanen, M. (2019). Johdatus tiedusteluun. Sähköinen kirja. Alma Talent Oy.

Lombardi, M., Rosenblum, T. & Burato A. (2015). From SOCMINT to Digital HUMINT: Re-frame the Use of Social Media Within the Intelligence Cycle. Fondazione De Gasperi. Haettu 4.3.2020 osoitteesta http://www.fondazionedegasperi.org/wp-content/uploads/2016/04/SocmInt-HumInt.pdf

Moseley, A. (n.d). Just War Theory. Haettu 26.2.2020 osoitteesta https://www.iep.utm.edu/justwar/#H5

Olcott, A. (2012). Open Source Intelligence in a Networked World. London: Continuum International Pub.

Omand, D. (2015). Understanding Digital Intelligence and the Norms That Might Govern It. GCIG Paper No. 8. Series: Global Commission on Internet Governance Paper Series. Haettu 4.3.2020 osoitteesta

https://www.cigionline.org/publications/understanding-digital-intelligence-and-norms-might-govern-it?utm_source=Newsletter&utm_medium=Web%20Archive&utm_campaign=CIGI%20WorldWide

OSINT Framework. (n.d.). Haettu 9.3.2020 osoitteesta https://osintframework.com/

Porvali, M. (2018). Tiedustelun näkymätön historia: Antiikista maailmansotiin. Atena Kustannus Oy. Painettu EU:ssa 2018.

Prunckun, H. (2013). Intelligence and Private Investigation : Developing Sophisticated Methods for Conducting Inquiries. Springfield, Illinois : Charles C. Thomas, Publisher, Ltd.

Putting Data in Perspective With Web Intelligence. 2014. Recorded Future. Haettu 14.4.2020 osoitteesta https://www.recordedfuture.com/web-intelligence-perspective/

Richelson, J. (2013). The Snowden Affair. National Security Archive Electronic Briefing Book No. 436. Haettu 4.3.2020 osoitteesta https://nsarchive2.gwu.edu/NSAEBB/NSAEBB436/

Saaranen-Kauppinen, A. & Puusniekka, A. (2006). KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. Haettu 4.9.2020 osoitteesta https://www.fsd.tuni.fi/menetelmaopetus/kvali/L7_3_5.html

Şuşnea, E. & Iftene, A. (2018). The Significance of Online Monitoring Activities for the Social Media Intelligence (SOCMINT). Proceedings of the Conferenceon Mathematical Foundations of InformaticsMFOI'2018, July 2-6, 2018, Chisinau, Republic of Moldova. Haettu 4.3.2020 osoitteesta https://ibn.idsi.md/sites/default/files/imag_file/MFOI-2018_0.pdf#page=230

Tolppanen, E. (2020). Opinnäytetyö. Avointen lähteiden tiedustelu ja henkilöprofilointi. Savonia-ammattikorkeakoulu: Tekniikan ja liikenteen ala. Haettu 5.9.2020 osoitteesta https://www.theseus.fi/bitstream/handle/10024/342850/Tolppanen_Eemeli.pdf?sequence=2&isAllowed=y

Tuomi, J. & Sarajärvi, A. (2018). Laadullinen tutkimus ja sisällönanalyysi. Uudistettu laitos. Helsinki: Kustannusosakeyhtiö Tammi.

Tuominen, S. (2019). Bachelor's Thesis. Open Source Intelligence and OSINT Applications. Oulu University of Applied Sciencies: Information Technology. Haettu 5.9.2020 osoitteesta

https://www.theseus.fi/bitstream/handle/10024/171315/Tuominen_Sanna.pdf?sequence=2&isAllowed=y

Vaskin, P. (2018). Opinnäytetyö. Sisäänrakennettu yksityisyyden suoja avointen lähteiden Internet-tiedustelussa. Laurea-ammattikorkeakoulu: Tietojenkäsittelyn koulutusohjelma, Tradenomi. Haettu 5.9.2020 osoitteesta https://www.theseus.fi/bitstream/handle/10024/159091/Petteri_Vaskin.pdf?sequence=1&isAllowed=y

Williams, H. & Blum, I. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defence Enterprise. RAND Corporation. Haettu 3.1.2020 osoitteesta https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf

Zeng, D., Chen, H., Lusch, R. & Li, S-H. (2010). Social Media Analytics and Intelligence. IEEE Intelligent Systems ( Volume: 25 , Issue: 6 , Nov.-Dec. 2010 ). Haettu 3.3.2020 osoitteesta https://ieeexplore.ieee.org/abstract/document/5678581/authors