Pinja Tervonen

Viranomaisten oma-aloitteinen tietojen antaminen hybridiuhkien torjumiseksi

Keskiössä tiedusteluviranomaisten toimivaltuudet

Johtamisen akateeminen yksikkö
Julkisoikeus, pro gradu -tutkielma
Hallintotieteiden maisteri

Vaasa 2024

VAASAN YLIOPISTO
Johtamisen akateeminen yksikkö
Tekijä: Pinja Tervonen
Tutkielman nimi: Viranomaisten oma-aloitteinen tietojen antaminen hybridiuhkien torjumiseksi: Keskiössä tiedusteluviranomaisten toimivaltuudet
Tutkinto: Hallintotieteiden maisteri
Oppiaine: Julkisoikeus
Työn ohjaaja: Kristian Siikavirta
Valmistumisvuosi: 2024 **Sivumäärä:** 114

TIIVISTELMÄ:
Turvallisuusympäristömme jatkuva muutos mahdollistaa erilaisten turvallisuusuhkien ilmenemisen. Erityisesti hybridiuhat, joissa hyödynnetään monenlaisia ja toistaan tukevia vaikuttamiskeinoja, ovat nousseet merkittäväksi uhaksi kansalliselle turvallisuudellemme. Viime vuosina eri viranomaisten toimivaltuuksista säätäviä lakeja on muutettu, jotta viranomaiset pystyisivät paremmin vastaamaan hybridiuhkiin. Myös vuonna 2019 voimaan tulleet tiedustelulait siviili- ja sotilastiedustelun toteuttamisesta pyrkivät omalta osaltaan vastaamaan hybridiuhkien synnyttämiin haasteisiin ja havainnoimaan Suomen kansalliseen turvallisuuteen ja maanpuolustukseen kohdistuvia uhkia.

Tässä tutkielmassa tarkastellaan tiedusteluviranomaisten oma-aloitteista tietojen antamista hybridiuhkien torjumiseksi ja pyritään jäsentelemään ne säännökset, joiden pohjalta tiedusteluviranomainen voi antaa tiedustelumenetelmin hankkimaansa tietoa oma-aloitteisesti toiselle viranomaiselle tai muulle taholle. Tutkielmassa keskitytään oma-aloitteiseen tietojen antamiseen sellaisesta tiedustelumenetelmin hankitusta tiedosta, joka viittaa hybridiuhkaan. Tutkielmassa selvitetään tiedusteluviranomaisten toimivaltuudet hankkia tietoa hybridiuhan osatekijöistä sekä edellytykset tällaisen tiedon antamiseen oma-aloitteisesti.

Tutkielma on metodiltaan oikeusdogmaattinen eli lainopillinen. Lainoppi tutkii voimassa olevaa oikeutta ja sen tavoitteena on luoda jäsennelty kuva voimassa olevista oikeusnormeista. Hybridiuhkien ollessa monimutkaisia turvallisuusuhkia, myös toimivaltuudet niiden torjumiseksi voivat kuulua useille eri viranomaisille. Lisäksi tiedusteluviranomaisten oma-aloitteisesta tietojen antamisesta on säädetty monissa eri laeissa. Sen vuoksi tutkielmassa systematisoidaan tiedusteluviranomaisen oma-aloitteista tietojen antamista koskevat säännökset jäsennellyksi kokonaisuudeksi ja suhteutetaan ne tiedusteluviranomaisten toimivaltuuksiin hybridiuhkien torjumiseksi. Tutkielman aineistona hyödynnetään voimassa olevien säädösten lisäksi lakien valmisteluasiakirjoja, oikeuskirjallisuutta, kansallisia ja kansainvälisiä oikeustapauksia, kansallisten laillisuusvalvojien ratkaisuja sekä erilaisia valtioneuvoston selontekoja.

Tutkielma osoittaa, että tiedusteluviranomaisilla on lähtökohtaisesti kattavat toimivaltuudet sekä tiedon hankintaan eri hybridiuhkan keinoista että tällaisen hybridiuhkaan viittaavan tiedustelutiedon oma-aloitteiseen antamiseen toisille viranomaisille tai muille tahoille. Kyseisten viranomaisten toimivaltuuksien tulee olla täsmällisesti kirjattuna lakiin. Lainsäädäntö on kuitenkin hidas väline nopeasti muuttuvien hybridiuhkien uusiin keinoihin vastaamiseksi, eikä kaikkia tulevaisuuden uhkia ole voitu tiedustelulakeja säädettäessä ennakoida. Näin ollen lainsäädännön lisäksi erityiseen asemaan hybridiuhkien torjunnassa nousevat muut keinot ja välineet, kuten kattava sektorikohtainen, mutta myös sektorirajat ylittävä varautuminen ja eri toimijoiden välinen yhteistyö.

AVAINSANAT: hybridivaikuttaminen, hybridiuhat, tiedustelu, kansallinen turvallisuus, maanpuolustus, salassapitovelvollisuus, viranomaisyhteistyö

Sisällys

1 Johdanto 6
1.1 Johdatus aiheeseen 6
1.2 Tutkielman tavoitteet ja tutkimuskysymykset 10
1.3 Tutkimusmenetelmät ja tutkielman aineisto 13
1.4 Rakenne ja tutkimuksen eteneminen 17
2 Tiedusteluviranomaisten toimivaltuudet torjua hybridiuhkia 19
2.1 Hybridiuhat, hybridivaikuttaminen ja hybridisodankäynti 19
2.1.1 Keinoja hybridiuhkien synnyttämiseksi 25
2.1.2 Uhkia aiheuttavat toimijat ja uhkatoimien oikeudellinen arviointi 30
2.2 Tiedusteluviranomaiset ja tiedustelulainsäädännön mukaiset toimivaltuudet 33
2.2.1 Tiedustelun tarkoitus 34
2.2.2 Tiedustelumenetelmät 37
2.2.3 Tiedustelutoimivaltuudet hybridiuhkien torjumiseksi 42
3 Oma-aloitteinen tietojen antaminen hybridiuhkien torjumiseksi 49
3.1 Viranomaisten oma-aloitteinen tietojen antaminen 49
3.1.1 Yleinen tietojen antaminen 53
3.1.2 Erityinen tietojen antaminen 57
3.2 Tiedustelumenetelmin saadun tiedon antaminen hybridiuhkan torjumiseksi 62
3.2.1 Tiedustelutiedon antaminen toimivaltaiselle viranomaiselle 65
3.2.2 Tiedustelutietojen antaminen rikostorjuntaviranomaisille 74
3.2.3 Tiedustelumenetelmin saatujen henkilötietojen antaminen 80
4 Yksityisyyden suoja tiedustelutoiminnassa ja viranomaisten työn tuloksellisuus 84
4.1 Yksityisyyden suojan huomioiminen tiedustelutoiminnassa 86
4.2 Viranomaisten välinen tietojenvaihto ja viranomaisen työn tehokkuus 91
5 Johtopäätökset 95
Lähteet 105

Kuviot

Kuvio 1. Hybridiuhan käsite. 22

Kuvio 2. Hybridivaikuttamisen ja hybridisodankäynnin erilaisia keinoja. 29

Kuvio 3. Tiedusteluviranomaisten tiedonhankintatoimivaltuudet hybridiuhkan osatekijöistä. 48

Kuvio 4. Tiedusteluviranomaisten oma-aloitteista tietojen antamista koskevat säännökset käyttötarkoituksittain. 98

Lyhenteet

EIS	Euroopan ihmisoikeussopimus
EIT	Euroopan ihmisoikeustuomioistuin
EU	Euroopan unioni
EUT	Euroopan unionin tuomioistuin
EOA	Eduskunnan oikeusasiamies
HaVL	Hallintovaliokunnan lausunto
HaVM	Hallintovaliokunnan mietintö
HE	Hallituksen esitys eduskunnalle
HL	Hallintolaki (434/2003)
JulkL/julkisuuslaki	Laki viranomaisten toiminnan julkisuudesta (621/1999)
KHO	Korkein hallinto-oikeus
Nato	Pohjois-Atlantin puolustusliitto
OKV	Valtioneuvoston oikeuskansleri
PeVL	Perustuslakivaliokunnan lausunto
PeVM	Perustuslakivaliokunnan mietintö
PL	Suomen perustuslaki (731/1999)
PuVM	Puolustusvaliokunnan mietintö
PolHalL	Laki poliisin hallinnosta (110/1992)
PolHetiL	Laki henkilötietojen käsittelystä poliisitoimessa (616/2019)
PolL	Poliisilaki (872/2011)
RL	Rikoslaki (39/1889)

SKRTL	Laki sotilaskurinpidosta ja rikosten torjunnasta puolustusvoimissa (255/2014)
SopS	Suomen säädöskokoelman sopimussarja
SotTiedL	Laki sotilastiedustelusta (590/2019)
Supo	Suojelupoliisi
TP-UTVA	Ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteinen kokous
TtStL	Laki tietoliikennetiedustelusta siviilitiedustelussa (582/2019)
vp	Valtiopäivät
YK	Yhdistyneet kansakunnat
YTS	Yhteiskunnan turvallisuusstrategia

1 Johdanto

1.1 Johdatus aiheeseen

Kansainvälisen kehityksen viimeaikainen yllätyksellisyys on asettanut turvallisuus- ja toimintaympäristömme jatkuvan muutoksen kohteeksi. Yllätykselliset tapahtumat saavat aikaan uudenlaisia uhkia, joita voi olla vaikea tunnistaa ja ennakoida. Muuttuvat uhkat ja uhkakuvat muuttavat turvallisuuskäsitystämme ja lisäävät tarvetta uudenlaisille keinoille uhkiin vastaamiseksi. Muutosnopeutta ja ennakoinnin vaikeutta hyödyntävä hybridivaikuttaminen kohdistuu yhteiskunnan eri osa-alueisiin laaja-alaisesti, kuitenkaan ylittämättä sodankäynnin kynnystä[1]. Hybridivaikuttamisessa ja siitä johtuvissa hybridiuhissa on kyse monenlaisten keinojen yhdistämisestä ja sen tavoitteena on horjuttaa yhteiskunnan poliittisia, taloudellisia, sotilaallisia, informatiivisia ja infrastruktuurisia rakenteita[2]. Hybridivaikuttamisen keinoja ovat esimerkiksi informaatiovaikuttaminen ja kyberhyökkäykset, poliittiset, taloudelliset ja sotilaalliset keinot kuten tunnuksettomien sotilaiden käyttäminen sekä muuttoliikkeen hyödyntäminen laajamittaisen maahantulon välineenä. Hybridivaikuttaminen voi sisältää sinänsä laillisiakin keinoja, mikä osaltaan vaikeuttaa hybridivaikuttamisen tunnistamista.[3] Tällaista monitahoista hybridivaikuttamista on usein hankala huomata, mikä tekee siihen puuttumisesta ja varautumisesta haastavaa.

Viranomaisten mahdollisuuksia hybridivaikuttamiseen ja -uhkiin vastaamiseksi on parannettu viime vuosien aikana muun muassa valmiuslain (1552/2011, muutettu lailla 706/2022) muuttamisella heinäkuussa 2022, jonka myötä valmiuslainsäädäntö huomioi nykyään kattavammin erilaiset hybridiuhat ja säätää niihin käytettävissä olevista häiriö- ja poikkeustilanteiden toimivaltuuksista[4]. Samoin aluevalvontalain (755/200, muutettu lailla 502/2017) ja rajavartiolain (578/2005, muutettu lailla 698/2022) muuttamisella on

[1] Björn ja Puistola, 2023, s. 18.
[2] Turvallisuuskomitea, 2016, s. 3.
[3] HE 63/2022 vp, s. 4.
[4] HE 63/2022 vp, s. 1.

osaltaan parannettu hybridiuhkiin vastaamista erityisesti tunnuksettomien sotilaiden toimintaan ja välineellistettyyn maahantuloon vastaamiseksi. Lisäksi hybridiuhkien kannalta merkittävä lainsäädäntöuudistus on vuonna 2019 voimaan tullut tiedustelulainsäädäntökokonaisuus, joka sisältää erilliset säädökset suojelupoliisin harjoittamasta siviilitiedustelusta ja Puolustusvoimien suorittamasta sotilastiedustelusta, joiden avulla pyritään torjumaan sotilaalliseen maanpuolustukseen ja kansalliseen turvallisuuteen kohdistuvia uhkia. Siviilitiedustelusta säädetään poliisilain (872/2011) 5 a luvussa lain poliisilain muuttamisesta (581/2019) mukaisesti sekä laissa tietoliikennetiedustelusta siviilitiedustelussa (582/2019). Sotilastiedustelusta sen sijaan säädetään laissa sotilastiedustelusta (590/2019). Nämä säädökset antavat kansalliselle tiedustelutoiminnalle raamit ja osaltaan edistävät hybridiuhkien torjumista.

Vaikka lainsäädäntöä on jo muutettu vastaamaan paremmin nykyistä turvallisuustilannettamme, on lainsäädännön päivittämiselle ja viranomaisten tehokkaammille toimivaltuuksille hybridiuhkien torjumiseksi yhä tarvetta. 20.6.2023 julkaistussa pääministeri Petteri Orpon hallitusohjelmassa toimiksi on nostettu sekä tiedustelu- että valmiuslainsäädännön päivittäminen, jotta mahdollistetaan hybridiuhkien tehokkaampi torjunta[5]. Koska tiedustelulainsäädännön päivittäminen on tunnistettu tarpeelliseksi, onkin ajankohtaista tutkia, miten tiedustelutoimivaltuudet tällä hetkellä mahdollistavat hybridiuhkien torjunnan ja onko toimivaltuuksissa puutteita. Samalla on hyvä pohtia tiedusteluviranomaisten toimivaltuuksia oma-aloitteiseen tietojen antamiseen hybridiuhkia koskien ja siten viranomaisten välisen yhteistyön keinoihin tiedustelutoiminnassa.

Kesällä 2023 julkaistussa Viranomaisten oma-aloitteinen tietojenvaihto (Virvotieto) -hankkeen loppuraportissa nostettiin esiin siviilitiedustelua toteuttavan suojelupoliisin huoli tiedustelulakeihin kirjatun palomuurisääntelyn epäselvyydestä koskien tietojen

[5] Valtioneuvosto, 2023b, s. 167. Lisäksi sisäministeriö on 21.12.2023 asettanut säädöshankkeen (SM061:00/2023) siviilitiedustelulainsäädännön ja suojelupoliisin tiedonvaihtoa koskevan lainsäädännön tarkistamiseksi. Hankkeen tavoitteena on arvioida palomuurisääntelyn, henkilötietojen luovuttamista kansainvälisessä yhteistyössä koskevan sääntelyn ja PL 10 §:n ajantasaisuus ja tarkistaminen. Myös sotilastiedustelusta annetun lain päivittämistä koskeva hanke on valmisteilla puolustusministeriössä, mutta siitä ei ole vielä annettu säädöshankepäätöstä. (Sisäministeriö, 2023b).

luovuttamista rikostorjuntaviranomaiselle hybridiuhkien torjumiseksi[6]. Suojelupoliisista nostettiin esiin, että tiedustelumenetelmän avulla voidaan saada selville sellaista tietoa, joka olisi välttämätöntä luovuttaa rikostorjuntaviranomaiselle esimerkiksi konkreettisen hybridiuhkan torjumiseksi, mutta nykyinen käytäntö tämänkaltaisesta tietojen antamisesta on epäselvä[7]. Tiedustelulakien palomuurisäännöksissä säädetään rikosta koskevien tietojen luovuttamisesta rikostorjuntaviranomaisille, sillä säännösten tarkoituksena on osaltaan estää tiedon hankkiminen tiedustelumenetelmin rikostorjuntaan. Vaikka suojelupoliisin esimerkissä kyse on tiedon luovuttamisesta nimenomaan rikostorjuntaviranomaiselle, tarpeellista on kuitenkin selvittää, onko tämänkaltainen tietojen antaminen hybridiuhkaan viittaavasta tiedosta mahdollista toiselle viranomaiselle nykyisten toimivaltuuksien nojalla erityisesti viranomaisten toiminnan julkisuudesta annetun lain (621/1999, myöhemmin julkisuuslaki tai JulkL) tai tiedusteluviranomaisten toiminnasta säätävien erityislakien säännösten nojalla. Tulen myös pohtimaan palomuurisääntelyä ja sen tulkintoja tietojen antamisesta rikostorjuntaviranomaiselle.

Mikä sitten on uhka ja erityisesti hybridiuhka? Uhkat ovat aikaan ja paikkaan sidoksissa ja siksi nykypäivän uhkat ovat hyvin erilaisia kuin muutama vuosikymmen sitten[8]. Maailman kehittymisen lisäksi eri toimijat havainnoivat ja määrittelevät uhkia eri tavalla, sillä yksilöä uhkaa useimmiten erityyppiset asiat kuin valtiota, vaikka lopulta valtioon kohdistuvat uhkat vaikuttavat myös yksilöön. Lisäksi uhkat näyttäytyvät eri tavalla eri valtioissa, sillä erilaiset uhkat saavat toisissa valtioissa enemmän painoarvoa kuin toisissa.[9] Oikeudellisesti uhka määritellään usein rikolliseksi toiminnaksi, mutta Kokonaisturvallisuuden sanastossa uhka on määritelty haitalliseksi tapahtumaksi tai kehityskuluksi, jonka toteutuminen on vielä epävarmaa, mutta mahdollista[10]. Kansalliseen turvallisuuteen kohdis-

[6] Kurvinen ja muut, 2023, s. 159. Palomuurisääntely rajoittaa tiedusteluviranomaisen tiedonanto-oikeutta ja säätää siitä, millaisin edellytyksin rikoksia koskevaa tietoa saa, ei saa ja pitää luovuttaa rikostorjuntaviranomaisena toimivalle poliisille tai muulle esitutkintaviranomaiselle. (Valtioneuvosto, 2021b, s. 23.) Ks. myös EOAK/289/2021.
[7] Kurvinen ja muut, 2023, s. 159.
[8] Iloniemi & Limnéll, 2018, s. 14.
[9] Seppälä, 2011, s. 1–2.
[10] Kokonaisturvallisuuden sanasto, 2017, s. 40.

tuva uhka sen sijaan on toimi tai tapahtumasarja, joka uhkaa merkittävällä tavalla kansalaisten elämänlaatua tai valtion olemassa olevia poliittisia vaihtoehtoja[11]. Uhka on siis jotain epätoivottua toimintaa, jota yleisesti pidetään vääränä tai pahana[12].

Uhka voi saada alkunsa teknisistä syistä, olosuhteiden muutoksesta tai ihmisen tarkoituksellisesta tai tarkoituksettomasta toiminnasta[13]. Vuoden 2017 Yhteiskunnan turvallisuusstrategiassa nykypäivän uhkat nähdään nopeasti muuttuvina, arvaamattomina ja kestoltaan vaihtelevina, ja ne voivat ilmetä itsenäisinä, samanaikaisina tai toistensa jatkumoina[14]. Tällaisia monimutkaisia uhkia on vaikea ennustaa ja samalla myöskään kaikkia mahdollisia vaikuttamisen keinoja ei voida etukäteen tunnistaa. Monimutkaisia uhkia ja keinoja hyödyntävällä hybridivaikuttamisella pyritään keinojen yhteisvaikutuksen myötä vaikuttamaan yhteiskunnan haavoittuviin toimintoihin, kuten kriittiseen infrastruktuuriin ja päätöksentekoon[15]. Hybridivaikuttaminen onkin joko valtiollisen tai ei-valtiollisen tahon tietoista toimintaa, jolla pyritään saavuttamaan omat tavoitteet ja heikentämään vaikuttamisen kohdetta useita, toisiaan täydentäviä vaikuttamiskeinoja käyttäen[16]. Hybridiuhka on ilmentymä näiden vaikuttamiskeinojen käytöstä[17]. Hybridiuhka on mahdollista valtioon kohdistuvaa haitallista toimintaa, joka konkretisoituu todelliseksi uhkaksi, kun erilaisia keinoja yhdistelevä vaikuttamistoiminta muuttuu aktiiviseksi.

Hybridiuhkista puhuttaessa keskitytään nimenomaan valtiota uhkaaviin toimiin tai tapahtumiin, sillä ne pyritään tavoitteellisesti suuntaamaan yhteiskunnan haavoittuviin toimintoihin. Hybridiuhka toteutuessaan synnyttää yhteiskunnassa häiriötilanteen, joka YTS:n mukaan aiheutuu tapahtumasta tai uhkasta, joka vaarantaa yhteiskunnan elintärkeitä toimintoja tai strategisia tehtäviä[18]. Hybridiuhat ovat siis tarkoituksellisia, strategisesti suunniteltuja toimia, minkä vuoksi esimerkiksi luonnonilmiöstä johtuva katkos

[11] Lonka ja muut, 2020, s. 29.
[12] Helsingin kaupunki, 2018, s. 6.
[13] Sisäministeriö, 2023a, s. 12.
[14] Yhteiskunnan turvallisuusstrategia, 2017, s. 25.
[15] Iloniemi & Limnéll, 2018, s. 22.
[16] Kokonaisturvallisuuden sanasto, 2017, s. 46; Helsingin kaupunki, 2018, s. 5.
[17] Helsingin kaupunki, 2018, s. 5.
[18] Yhteiskunnan turvallisuusstrategia, 2017, s. 97.

energianjakelussa ei ole hybridiuhka, vaikkakin se on häiriötilanne. Toisaalta tällaista häiriötilannetta voidaan hyödyntää hybridivaikuttamisessa, jolloin häiriötilanteeseen johtanutta heikkoutta käytetään hyväksi muulla tavoin häiriötilanteen aikana tai valmistauduttaessa tulevaisuuden hybridivaikuttamiseen[19].

Monitahoisten ja monimutkaisten hybridiuhkien torjuminen ja estäminen vaatii niin viranomaisten, päättäjien, kuntien, hyvinvointialueiden ja maakuntien, yksityisen ja kolmannen sektorin kuin kansalaistenkin yhteistoimintaa, jota Suomessa toteutetaan kokonaisturvallisuuden yhteistoimintamallilla[20]. Toimenpiteitä hybridiuhkien torjumiseksi toteutetaan yhteisesti myös EU:n laajuisesti, minkä lisäksi Suomen liittyminen keväällä 2023 puolustusliitto Naton jäseneksi tuo uuden kansainvälisen yhteistyöelimen turvallisuuskenttäämme. Kuitenkin viranomaisten tiedustelutoiminnalla ja kansainvälisellä tiedusteluyhteistyöllä on suuri merkitys hybridiuhkien torjunnassa ja tunnistamisessa[21], joten keskityn tässä tutkielmassa nimenomaan tiedusteluviranomaisten väliseen yhteistyöhön ja erityisesti tiedustelutietojen antamiseen toisille viranomaisille tai muille toimijoille hybridiuhkien torjumiseksi.

1.2 Tutkielman tavoitteet ja tutkimuskysymykset

Tämän tutkielman tavoitteena on selvittää, onko tiedusteluviranomaisilla riittävät toimivaltuudet torjua hybridiuhkia erityisesti oma-aloitteisen tietojen antamisen avulla. Tarkastelen tiedusteluviranomaisten toimivaltuuksia voimassa olevan tiedustelulainsäädännön pohjalta sekä pyrin selvittämään, voivatko tiedusteluviranomaiset nykyisillä toimivaltuuksillaan antaa oma-aloitteisesti tietoa toiselle viranomaiselle, kun kyseessä on tiedustelumenetelmin saatu tieto, joka viittaa hybridivaikuttamiseen tai -uhkaan. Viranomaisten oma-aloitteista tietojen antamista käsitellään myös hallinto-oikeudellisesta näkökulmasta ja pyrin selvittämään, antaako jokin muu säännös tiedusteluviranomaisille

[19] Sisäministeriö, 2023a, s. 26.
[20] Yhteiskunnan turvallisuusstrategia, 2017, s. 7.
[21] Valtioneuvosto, 2022, s. 29.

toimivaltuuden oma-aloitteiseen tietojen antamiseen hybridiuhkan torjumiseksi, jos tiedustelulainsäädäntö ei sitä anna. Tutkielma on siis osittain hallinto-oikeudellinen sekä informaatio-oikeudellinen.

Tutkielman ensimmäisenä tavoitteena on selvittää ja kuvata tiedustelulakien mukaiset tiedusteluviranomaisten toimivaltuudet torjua hybridiuhkia. Tutkielmani ensimmäisenä tutkimuskysymyksenä on; *Miten tiedusteluviranomaiset voivat torjua hybridiuhkia tiedustelulakien mukaisilla toimivaltuuksilla?* Toinen tavoite on selvittää, voidaanko hybridiuhkia torjua voimassa olevan lainsäädännön mukaan viranomaisten oma-aloitteisen tietojen antamisen avulla tiedusteluviranomaisten toimesta. Toinen tutkimuskysymykseni on; *Miten hybridiuhkia voidaan torjua viranomaisten oma-aloitteisen tietojen antamisen avulla ja onko tiedusteluviranomaisilla riittävät toimivaltuudet oma-aloitteiseen tietojen antamiseen eri viranomaisille hybridiuhkien torjumiseksi?* Viimeisenä tutkielmassa tarkastellaan lyhyesti yksityisyyden suojan toteutumista tiedustelutoiminnassa ja onko tiedustelutoiminnalla saadun tiedon antaminen oikeutettua viranomaisen työn tuloksellisuudella tai tehokkuudella perustellen.

Rajaan tutkimukseni koskemaan hybridiuhkien, hybridivaikuttamisen ja hybridisodankäynnin torjumista koskevia toimivaltuuksia ja tietojen antamista tiedusteluviranomaisten toimesta. Viranomaisten tietojen antamisesta säädetään yleisesti julkisuuslaissa, jonka 1 §:n mukaan viranomaisen asiakirjat ovat lähtökohtaisesti julkisia, jolloin asiakirjojen tiedon saa antaa toiselle viranomaiselle. Julkisuusperiaate pätee kaikkiin viranomaisen asiakirjoihin, jollei julkisuuslaissa tai muussa laissa säädetä asiakirjan sisältämien tietojen salassapidosta. Salassa pidettäväksi määrättyä asiakirjaa tai tietoa asiakirjan sisällöstä sen sijaan ei saa antaa sivulliselle julkisuuslain 22 §:n mukaisesti ja säännöksessä tarkoitetuksi sivulliseksi katsotaan myös toiset viranomaiset[22]. Näin ollen viranomaisilla ei ole yleistä oikeutta saada tietoa toisen viranomaisen asiakirjasta, vaan oikeus

[22] Mäenpää, 2020, s. 248.

tiedon saamiseen tai antamiseen salassa pidettävästä asiakirjasta määräytyy laintasoisella säännöksellä[23]. Julkisuuslain 3 §:n mukaan laissa säädettyjen tiedonsaantioikeuksien ja viranomaisten velvollisuuksien, mukaan lukien tiedonantovelvollisuuksien, tarkoituksena on muun muassa viranomaisten toiminnan avoimuuden toteuttaminen. Koska julkisten viranomaisen hallussa olevien tietojen antaminen on yleinen lähtökohta, keskitytään tässä tutkielmassa salassa pidettävien tietojen antamiseen tiedusteluviranomaisen toimesta ja pyritään kuvaamaan ne säännökset, jotka mahdollistavat tiedon antamisen oma-aloitteisesti.

Viranomaisten välisestä tietojenvaihdosta säädetään julkisuuslain lisäksi monissa erityislaeissa, minkä vuoksi asiaa ei ole mielekästä käsitellä tässä tutkimuksessa useamman viranomaisen toimivaltaa käsittävällä laajuudella, vaan käsittely on rajattu tiedusteluviranomaisiin. Näistä erityislaeista tämän tutkimuksen kannalta keskeisimpiä ovat poliisilain 5 a luvun (581/2019), henkilötietojen käsittelystä poliisitoimessa annetun lain (616/2019), sotilastiedustelusta annetun lain (590/2019), henkilötietojen käsittelystä Puolustusvoimissa annetun lain (332/2019) ja tietoliikennetiedustelusta siviilitiedustelussa annetun lain (582/2019) tietojenvaihtoa ja tietojen antamista koskevat säännökset.

Viranomaisten välisen tietojenvaihdon voi ajatella olevan osa hallintolain (434/2003) 10 §:ssä säädettyä hyvän hallinnon perusteiden mukaista viranomaisten välistä yhteistyötä. Tästä yhteistyövelvoitteesta ei kuitenkaan voida johtaa yleistä viranomaisen tietojenantovelvollisuutta, vaan kyse on viranomaisten oman hallinnonalan tehtävien täyttämiseen kohdistuvasta yhteistyöstä, jossa viranomaiset toimivat omilla toimivaltuuksillaan salassapitovelvollisuutensa rajoissa[24]. Tutkimuksessa käsitellään siis viranomaisten välistä yhteistyötä tietojenvaihtoon ja oma-aloitteiseen tietojen antamiseen soveltuvin osin, mikäli sellaisia on, eikä tutkimuksessa siten käsitellä laajemmin viranomaisten välistä yhteistyötä taikka viranomaisten toisilleen antamaa virka-apua.

[23] Mäenpää, 2020, s. 250.
[24] Heuru, 2003, s. 310.

Hybridivaikuttaminen pyritään naamioimaan toiminnaksi, joka ei ylitä rikosoikeudellisesti arvioitavan toiminnan kynnystä, mutta hybridivaikuttamisen osana toteutettavat toimet voivat olla rikosoikeudellisen toimivallan piirissä. Esimerkiksi hybridivaikuttamisessa useimmiten hyödynnettävä kybervaikuttaminen voi olla luonteeltaan rikollista esimerkiksi silloin, kun huoltovarmuuskriittisten tai muuten yhteiskunnan kriittisten toimijoiden tietoverkkoa häiritään palvelunestohyökkäyksillä tai niiden tietojärjestelmiin asennetaan kiristyshaittaohjelmia tai kohdistetaan tietomurto[25]. Lisäksi hybridivaikuttamista voi tapahtua myös terroristi- tai rikollisjärjestöjen toimesta, tai niiden kautta, jolloin toiminta kuuluu kohdevaltion rikosoikeudellisen toimivallan piiriin[26]. Kuitenkaan tämän tutkielman tarkoituksena ei ole käsitellä tietojen antamista rikosten torjumisen näkökulmasta, koska tiedustelutoimivaltuuksia ei lähtökohtaisesti saa käyttää rikosten selvittämiseksi tai torjumiseksi[27]. Tämän vuoksi tutkimuksessa keskitytään tietojen antamiseen hybridiuhkien torjumiseksi eikä tietojen antamista käsitellä rikosten torjumiseen liittyen, jollei se ole tutkimuksen aiheen kannalta tarpeen esimerkiksi tiedustelulakien palomuurisääntelyä tarkasteltaessa.

1.3 Tutkimusmenetelmät ja tutkielman aineisto

Tutkielman ollessa julkisoikeudellinen tutkimus, käytän tutkielmassa oikeustieteellisenä tutkimusmetodina lainoppia eli oikeusdogmatiikkaa. Lainopin keskeisenä tehtävänä on tulkita ja systematisoida oikeussääntöjä eli oikeusnormeja[28]. Oikeusnormilla tarkoitetaan oikeudellisen tekstin merkityssisältöä, joka toimii tulkinnan kohteena[29]. Voimassa olevat oikeusnormit muodostavat oikeusjärjestyksen, joka on lainopillisen tutkimuksen

[25] Valtioneuvosto, 2023a, s. 13. Rikoslain (39/1889) 38 luvun säännökset säätävät erilaisista tieto- ja viestintärikoksista, joista kyseisissä tapauksissa voi tulla sovellettavaksi esimerkiksi 5-8a § koskien tietoliikenteen häirintää, tietojärjestelmän häirintää ja tietomurtoa. Ks. myös Euroopan neuvoston tietoverkkorikollisuutta koskeva Budapestin yleissopimus, 23.11.2001, CETS N:o 185 ja siihen annettu toinen lisäpöytäkirja tiiviimmästä yhteistyöstä ja sähköisen todistusaineiston luovuttamisesta, EUVL N:o L 63, 28.2.2023.
[26] Voimankäytön oikeussäännöt, 2015, s. 39.
[27] HE 202/2017 vp, s. 182; HE 203/2017 vp, s. 320.
[28] Aarnio, 1997, s. 36–37.
[29] Määttä, 2016, s. 158.

kohde[30]. Näin ollen lainopin keinoin pyritään selvittämään tutkimuksen teon hetkellä voimassa olevan oikeusjärjestyksen sisältö oikeusnormien tulkinnan sekä oikeussäännösten systematisoinnin avulla[31]. Tarkoitukseni on lainopin keinoin tutkia hybridiuhkien torjumista tiedusteluviranomaisten toimivaltuuksien pohjalta sekä sitä, mahdollistaako voimassa oleva lainsäädäntö tiedusteluviranomaisten oma-aloitteisen tietojen antamisen toisille viranomaisille hybridiuhkien torjumiseksi.

Oikeudelliseen tekstiin jätetään usein harkinnanvaraa lainsoveltajalle, joten lainopin avulla tuotetaan tulkintaehdotuksia siitä, miten oikeudellinen ongelma tulisi tutkijan mielestä ratkaista[32]. Lisäksi lain säännökset on kirjoitettu aina yleiseen muotoon, jolloin lainopin tehtävänä on selvittää, miten säännös soveltuu tutkittavana olevaan käytännön tilanteeseen ja mitä kriteerejä lainsoveltajan on otettava tilanteessa huomioon[33]. Tulkinnan ohessa oikeusnormeista koostuvaa aineistoa systematisoidaan eli järjestetään selkeään ja mahdollisimman ristiriidattomaan järjestykseen[34]. Systematisoinnissa on siis kyse hajanaisista oikeuslähteistä kootun tiedon järjestämisestä johdonmukaiseksi kokonaisuudeksi[35].

Lainopissa oikeusnormien tulkinta ja systematisointi ovat keskinäisessä vuorovaikutussuhteessa toisiinsa, sillä tulkinnan avulla selvitetään oikeussäännön sisältämien oikeustosiseikkojen oikeudellisia seuraamuksia, kun taas systematisoinnin avulla pyritään täsmentämään niitä käsitteitä, joiden avulla suhde oikeustosiseikan ja oikeusseuraamuksen välillä pystytään tunnistamaan[36]. Aarnion mukaan oikeusnormien systematisoinnilla pyritään jäsentämään käsitteitä uudelleen, jotta oikeussäännöksiä on helpompi ymmärtää ja käyttää[37]. Systematisoimalla oikeussäännöksiä luodaan oikeudenalakohtaisia yleisiä

[30] Kaisto, 2005, s. 162.
[31] Kaisto, 2005, s. 344.
[32] Määttä, 2016, s. 151.
[33] Määttä, 2016, s. 149–150.
[34] Sajama, 2016, s. 40.
[35] Sajama, 2016, s. 41.
[36] Aarnio, 1997, s. 40.
[37] Aarnio, 1997, s. 43; Sajama, 2016, s. 41.

oppeja, kuten ratkaisuohjeita tarjoavia oikeusperiaatteita sekä oikeuskäsitteitä[38]. Yleisten oppien avulla tunnistetaan ja muotoillaan oikeusongelmia sekä niiden avulla perustellaan oikeudellisia päätöksiä viranomaisessa ja tuomioistuimessa[39]. Nämä yleiset opit ohjaavat osaltaan myös oikeusnormien tulkintaa, mikä näkyy tässä tutkielmassa hallinto-oikeuden oikeusperiaatteiden hyödyntämisellä oma-aloitteista tietojen antamista koskevien oikeussäännösten tulkinnassa.

Tutkimuksessa hyödynnetään lainopin menetelmiä, kuten oikeuslähdeoppia sekä tulkinta-, argumentaatio- ja punnintamenetelmiä. Menetelmien avulla pyritään tuottamaan tietoa voimassa olevasta oikeudesta ja antamaan siitä jäsennelty kokonaiskuva lainsoveltamisen tueksi. [40] Hybridiuhkien torjumista tarkastellaan tiedusteluviranomaisten toimivaltuuksien näkökulmasta ja tutkimuskohdetta lähestytään julkisoikeudellisten ja erityisesti hallinto-oikeudellisten oikeusperiaatteiden ja käsitteiden kautta. Tutkimus pohjautuu lainsäädäntöön ja sen velvoittavuuteen tiedusteluviranomaisten toiminnassa keskittyen erityisesti oma-aloitteiseen tietojen antamiseen hybridiuhkan torjumiseksi. Tutkimuksen tavoitteena on jäsentää tiedustelulakien mukaiset viranomaisten toimivaltuussäännökset ja oma-aloitteista tietojen antamista koskevat säännökset osaksi hybridiuhkien torjumisen oikeudellista keinovalikoimaa. Näin ollen tutkimuksen menetelmäksi sopii hyvin oikeusnormeja tulkitseva ja systematisoiva lainoppi.

Oikeusdogmatiikan eli lainopin tutkimuskohteena on voimassa oleva oikeus ja sen avulla on tarkoitus selvittää voimassa olevien oikeusnormien sisältöä oikeuslähteillä argumentoiden[41]. Oikeudellisessa ratkaisutoiminnassa oikeuslähteillä on kuitenkin toisiinsa nähden erilainen oikeuslähdearvo, jonka perusteella oikeuslähteet jaotellaan vahvasti velvoittaviin, heikosti velvoittaviin ja sallittuihin oikeuslähteisiin[42]. Aarnion mukaan vahvasti velvoittavia oikeuslähteitä ovat Suomen perustuslain perusoikeudet, kansalliset lait ja

[38] Kolehmainen, 2016, s. 128.
[39] Määttä & Paso, 2019, s. 12.
[40] Hirvonen, 2011, s. 55.
[41] Hirvonen, 2011, s. 21–22.
[42] Kolehmainen, 2016, s. 116.

niiden nojalla annetut alemman asteiset normit, kuten asetukset, kansallisen oikeuden osaksi saatetut kansainväliset sopimukset, eurooppaoikeuden normit, Euroopan ihmisoikeussopimuksen normit sekä Euroopan unionin tuomioistuimen (EUT) ja Euroopan ihmisoikeustuomioistuimen (EIT) tietyt prejudikaatit eli ennakkoratkaisut[43]. Vahvasti velvoittavan oikeuslähteen huomioimatta jättäminen tekee ratkaisusta lainvastaisen[44]. Aarnio jaottelee heikosti velvoittaviksi oikeuslähteiksi lainvalmisteluaineiston sekä kansallisten tuomioistuinten ennakkoratkaisut. Sallittuja oikeuslähteitä ovat Aarnion mukaan muun muassa yleiset oikeusperiaatteet, oikeustiede, eettiset ja moraaliset perusteet sekä taloudelliset, historialliset ja yhteiskunnalliset käytännölliset argumentit.[45] Heikosti velvoittavan oikeuslähteen sivuuttaminen asettaa ratkaisun tekijälle perusteluvelvollisuuden, kun taas sallitusta oikeuslähteestä poikkeaminen tai sen huomiotta jättäminen ei synnytä lainsoveltajalle seuraamuksia[46].

Näin ollen käytän tutkimusaineistona lainopille ominaisesti voimassa olevaa oikeutta eli lainsäädäntöä ja muita oikeuslähteitä, kuten lainvalmisteluasiakirjoja, oikeuskirjallisuutta ja tuomioistuinratkaisuja. Aineisto koostuu myös valtioneuvoston selonteoista, strategioista, tutkimusjulkaisuista ja ohjeista, joiden avulla pyritään kuvaamaan hybridiuhkan ja -vaikuttamisen käsitteitä ja torjumista, sillä ne eivät käsitteinä ole oikeudellisia, minkä vuoksi määrittelyä ei voida tehdä oikeuslähteiden pohjalta. Hybridivaikuttamisen ollessa kansainvälinen uhka, käytän aineistona myös kansainvälistä sääntelyä, kansainvälisiä sopimuksia ja raportteja. Lisäksi tutkielmassa hyödynnetään kansallisten lainvalvojien ratkaisuja ja asiantuntijalausuntoja. Lähdeaineisto sisältää monipuolisesti kaikkia oikeuslähdeopin mukaisia vahvasti ja heikosti velvoittavia sekä sallittuja oikeuslähteitä.

[43] Aarnio, 2006, s. 292.
[44] Kolehmainen, 2016, s. 116.
[45] Aarnio, 2006, s. 292.
[46] Kolehmainen, 2015, s. 116.

Sekä tiedusteluviranomaisten toimivaltuuksia että viranomaisten oma-aloitteista tietojen antamista on tutkittu kuluneen vuoden aikana, joten aihe on ajankohtainen kansallisessa tutkimuksessa. Tiedusteluviranomaisten tiedustelulainsäädännön mukaisia toimivaltuuksia hybridiuhkiin vastaamiseksi on tutkittu vuonna 2022 ilmestyneessä Saarikosken pro gradu -tutkielmassa[47], mutta oikeudellista tutkimusta aiheesta ei ole tehty. Valtioneuvoston selvitys- ja tutkimustoiminnassa[48] on tutkittu viranomaisten oma-aloitteista tietojen antamista rikosten torjumiseksi, josta julkaistiin raportti kesällä 2023. Kyseisen tutkimuksen osana julkaistiin Poliisiammattikorkeakoulun katsaus[49] viranomaisten tietojen antamisesta ja -vaihtamisesta, tiedonkulusta ja lainsäädännöstä muuttuneessa turvallisuus- ja toimintaympäristössä. Vaikka jälkimmäiseksi mainitussa katsauksessa on tutkittu aihetta muuttuneen turvallisuusympäristön näkökulmasta, ei raportissa ole sen syvemmin paneuduttu hybridivaikuttamisen ja -uhkien torjuntaan. Koska tiedustelulait velvoittavat tiedusteluviranomaisia turvaamaan toiminnallaan kansallista turvallisuutta, johon kohdistuvat uhkat voivat yhä useammin olla hybridiuhkia, on hyvä tutkia sitä, onko tiedusteluviranomaisilla riittävät toimivaltuudet tämän tehtävän hoitamiseen hybridiuhkatilanteessa.

1.4 Rakenne ja tutkimuksen eteneminen

Seuraavassa luvussa tarkastelen hybridivaikuttamista ja hybridiuhkia ja pyrin luomaan kokonaiskuvan hybridiuhkien laajuudesta sekä sijoittamaan nämä käsitteet osaksi oikeudellista keskustelua ja kontekstia. Kun olen määritellyt hybridivaikuttamisen ja hybridiuhat oikeudellisesti, siirryn tutkimaan tiedusteluviranomaisia ja niiden tiedustelulakien mukaisia tiedonhankintatoimivaltuuksia sekä sitä, miten näillä toimivaltuuksilla pystytään vastaamaan hybridiuhkiin. Tähän kysymykseen vastaamiseksi määrittelen ensin kotimaiset tiedusteluviranomaiset ja kuvaan niiden toimintaa ohjaavien tiedustelulakien

[47] Saarikoski, 2022.
[48] Kurvinen ja muut, 2023.
[49] Laitinen ja Kuukasjärvi, 2023.

keskeisen sisällön tämän tutkimuksen osalta. Tämän jälkeen tarkastelen tiedusteluviranomaisten toimivaltuuksia torjua hybridiuhkia, eli millaisia keinoja tiedusteluviranomaisilla on käytettävissä hybridiuhkien torjuntaan tiedustelulainsäädännön antamin toimivaltuuksin.

Kolmannessa luvussa siirryn tarkastelemaan viranomaisten välistä yhteistyötä oma-aloitteisen tietojen antamisen osalta. Aluksi kuvaan viranomaisten oma-aloitteista tietojen antamista yleisesti, jonka jälkeen siirryn tarkastelemaan tiedusteluviranomaisten mahdollisuuksia oma-aloitteiseen tietojen antamiseen toisille viranomaisille ja muille tahoille hybridiuhkien torjumiseksi. Koska tiedustelulainsäädäntö jakautuu siviili- ja sotilastiedustelua koskeviin erillisiin säädöksiin, tarkastelen tiedustelutoiminnalla saadun tiedon oma-aloitteista luovuttamista niin sotilas- kuin siviilitiedustelua koskevien erillisten säännösten osalta. Neljännessä luvussa tarkastelen vielä yksityisyyden suojan toteutumista tiedustelutoiminnassa ja miten yksityisyyden suoja vaikuttaa tiedonhankintaan hybridiuhista. Lisäksi tarkastelen, voidaanko tietoa antaa toiselle viranomaiselle viranomaisten työn tehokkuuden ja tuloksellisuuden nojalla.

2 Tiedusteluviranomaisten toimivaltuudet torjua hybridiuhkia

2.1 Hybridiuhat, hybridivaikuttaminen ja hybridisodankäynti

Ensimmäiseksi on syytä perehtyä hybridiuhkan käsitteeseen ja siihen liittyviin muihin käsitteisiin ja keinoihin, jotta ymmärrys tutkimuskysymyksistä ja tutkielman näkökulmasta täsmentyy. Kuten aiemmin olen todennut, hybridiuhilla ja hybridivaikuttamisella tarkoitetaan puhuttaessa lähes samaa toimintaa, sillä ne koostuvat laaja-alaisesta keinovalikoimasta, jota hyödyntämällä pyritään horjuttamaan yhteiskunnan toimintakykyä ja elintärkeitä toimintoja. Hybridiuhkaa ja hybridivaikuttamista kuvaavia kansainvälisesti hyväksyttyjä määritelmiä ei ole olemassa, mutta hybridiuhat voidaan nähdä eräänlaisena kattoterminä kaikelle monia keinoja yhdistävälle toiminnalle, joka uhkaa demokraattisten valtioiden toimintaa ja järjestelmiä[50]. Näin ollen voidaan ajatella, että hybridivaikuttaminen on toimintaa, joka muodostaa yhteiskuntaa uhkaavan hybridiuhkan.

Kansallisesti hybridiuhan ja hybridivaikuttamisen käsitteitä on määritelty esimerkiksi valmiuslakia (706/2022) ja rajavartiolakia (1311/2022) muutettaessa vuonna 2022 sekä tiedustelulakeja valmisteltaessa vuonna 2017, sillä säädöksillä pyritään edistämään viranomaisten mahdollisuuksia vastata yhteiskuntaan kohdistuviin turvallisuusuhkiin. Näiden lakien valmisteluaineistoissa hybridiuhka-käsitteen on viitattu tarkoittavan lähes poikkeuksetta hybridivaikuttamista, joka nähdään valtiota uhkaavana toimintana[51]. Hybridivaikuttaminen on suunnitelmallista toimintaa, jolla pyritään vaikuttamaan valtion heikkouksiin monia eri keinoja käyttäen toimijan omien tavoitteiden saavuttamiseksi[52]. Toimija voi olla vieras valtio tai muu ulkomainen toimija, joka erilaisia tehokkaita painostuskeinoja käyttäen pyrkii vaikuttamaan kohdevaltion poliittiseen, taloudelliseen ja sotilaalliseen päätöksentekoon tai infrastruktuurisiin rakenteisiin[53].

---

[50] Smith, 2019, s. 16.
[51] HE 203/2017 vp, s. 184 ja s. 124. Ks. myös HE 202/2017 vp, s. 155 ja s. 9 sekä HE 63/2022 vp, s. 4.
[52] HE 201/2017 vp, s. 5. Ks. myös HE 63/2022 vp, s. 4.
[53] HE 202/2017 vp, s. 10. Ks. myös HaVL 7/2018 vp, s. 16.

Hybridiuhkana pidetään sellaista yhteiskuntaan kohdistuvaa suunnitelmallisuutta, joka uhkasta käytännön toiminnaksi muuttuessaan on sellainen sisäisen tai ulkoisen turvallisuuden häiriötilanne, jonka torjuminen vaatii useamman kuin yhden viranomaisen toimivaltuuksia ja niiden välistä yhteistyötä[54]. Mielestäni voidaan ajatella, että hybridiuhka on yhteiskuntaan kohdistuva uhka tällaisen monitahoisen häiriötilanteen muodostumisesta, mutta siihen voidaan vastata vasta uhan konkretisoituessa varsinaiseksi häiriötilanteen synnyttämiseen tähtääväksi toiminnaksi, jota hybridivaikuttaminen on.

Tosin hybridiuhkien torjumisessa tärkeässä roolissa on hybridiuhkiin ja niiden synnyttämiin häiriötilanteisiin varautuminen ja ennakointi, missä apuna hyödynnetään muun muassa erilaisista uhkista laadittuja uhkamalleja ja niiden tueksi laadittuja uhka-arvioita, joiden pohjalta ryhdytään toimiin uhkan ehkäisemiseksi, torjumiseksi tai sen vaikutuksista selviämiseksi[55]. Varautuminen perustuu aina uhkamalleista ja -arvioista tehtävään riskiarvioon, mutta on tärkeää huomata, että kaikkia uhkia ei voida etukäteen riskiarviossa tunnistaa, vaan keskiössä on parantaa toimijoiden resilienssiä eli valmiutta toimia yllättävissä muutoksissa ja vahvistaa erilaisissa hybridivaikuttamisen ilmenemismuodoissa vaadittavia suorituskykyjä[56]. Tämän toteuttaminen edellyttää erityisesti huolellista lainsäädännön tarkastelua uusien riskiskenaarioiden tunnistamiseksi, jotta lainsäädäntöä voidaan muokata siten, etteivät vihamieliset toimijat voi hyödyntää lainsäädäntömme aukkoja käyttäessään eri vaikuttamiskeinoja[57]. Näin ollen hybridiuhkiin voidaan varautua nimenomaan hybridivaikuttamisen eri keinoihin varautuen.

Hybridiuhkan ja hybridivaikuttamisen lisäksi käytetään myös hybridioperaatioiden ja hybridisodankäynnin termejä, joilla viitataan samanlaiseen laaja-alaiseen vaikuttamistoimintaan, joka kohdistuu yhteiskunnan elintärkeisiin toimintoihin. Hybridiuhkista ja hybridisodankäynnistä puhutaan enemmän kansainvälisessä yhteisössä, kun taas kansalli-

[54] HE 94/2022 vp, s. 4.
[55] Kokonaisturvallisuuden sanasto, 2017, s. 41.
[56] Yhteiskunnan turvallisuusstrategia, 2017, s 25.
[57] Ferm, 2017, s. 6.

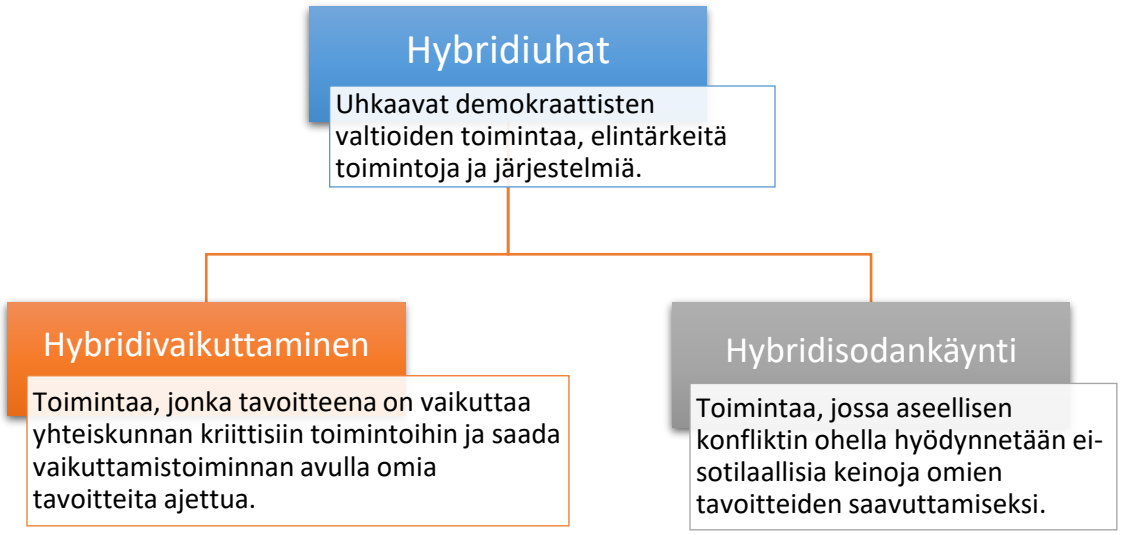
sesti käytetään usein hybridivaikuttamisen ja laaja-alaisen vaikuttamisen termejä. Mumford ja Carlucci ovat kuvanneet hybridisodankäynnin ja hybridiuhkien eroa siten, että hybridiuhat koostuvat laajasta valikoimasta väkivallattomia keinoja, joilla pyritään iskemään yhteiskunnan haavoittuviin toimintoihin ja heikentämään kohteiden toimintaa, yhtenäisyyttä ja tahdonvoimaa. Hybridisodankäynti sen sijaan on määritelty toiminnaksi, jossa voidaan yhdistää erilaisia sodankäynnin tyyppejä ja ei-sotilaallisia keinoja, joiden tavoitteena on neutralisoida tavanomaista sotilaallista voimankäyttöä.[58] Hybridisodankäynnin keinoja voivat olla tunnuksettomien sotilaiden käyttäminen, peiteoperaatiot ja epätavanomaisten taktiikoiden käyttäminen yhdistettynä perinteiseen aseelliseen konfliktiin[59]. Hybridisodankäynnissä pyritään siis tahallisesti hämärtämään rauhanajan ja sota-ajan eroa ja toimimaan tällä epäselvällä ”harmaalla alueella”[60].

Mumfordin ja Carluccin mukaan keskeinen ero on, että hybridisodankäynnissä yhdistetään sotilaallisia ja ei-sotilaallisia keinoja aseellisen konfliktin aikana, kun taas hybridiuhkissa tavoiteltu poliittinen vaikutus voidaan saavuttaa väkivallattomia keinoja käyttämällä ilman, että toiminta on osa aseellista konfliktia. Tärkeää on kuitenkin huomata, että myös sotilaallista voimaa voidaan käyttää väkivallattomasti, minkä vuoksi esimerkiksi asevoimat tai puolisotilaalliset joukot voivat synnyttää hybridiuhkia, mutta kyse ei kuitenkaan ole hybridisodankäynnistä.[61] Voidaan ajatella, että hybridisodankäynti on hybridiuhkaksi luokiteltavaa toimintaa, mutta hybridiuhka ei aina ole sidoksissa sodankäyntiin, sillä hybridiuhkana näyttäytyvä toiminta voi olla toteutettu myös hybridivaikuttamisen keinoin.

Myös kansallisesti on esitetty samansuuntaista tulkintaa, että hybridivaikuttaminen ei ole sidoksissa aseelliseen konfliktiin, sillä siinä hyödynnettävät toimet ovat tarkoitettu

[58] Mumford & Carlucci, 2023, s. 194.
[59] Voimankäytön oikeussäännöt, 2015, s. 38.
[60] Bajarūnas, 2020, s. 62.
[61] Mumford & Carlucci, 2023, s. 194.

niin tehokkaiksi, ettei aseelliseen hyökkäykseen ole tarpeellista ryhtyä[62]. Lisäksi valtioneuvoston puolustusselonteossa hybridivaikuttaminen ja siihen kytkeytyvä aseellinen voimankäyttö mielletään laaja-alaiseksi vaikuttamiseksi, jossa sotilaallisia keinoja voidaan pyrkiä käyttämään myös siten, että ne eivät täytä avoimen aseellisen konfliktin kynnystä, jolloin puolustajalla on käytössään vain normaaliolojen toimivaltuudet. Selonteon mukaan laaja-alainen vaikuttaminen on sotilaallinen uhka ja se kohdistuu maanpuolustukseen.[63] Ymmärränkin käsitteet siten, että hybridiuhka käsitteenä kattaa sekä hybridivaikuttamisessa että hybridisodankäynnissä hyödynnettävät erilaiset toimet, joilla tavoitellaan kohdemaan päätöksenteon ja rakenteiden horjuttamista aiheuttamalla monitahoisia häiriötilanteita. Toimet pyritään toteuttamaan siten, että ne eivät ylitä sodankäynnin tai poikkeusolojen käyttöönoton kynnystä, minkä vuoksi hybridiuhkiin pyritään ja joudutaan ensisijaisesti vastaamaan viranomaisten normaaliolojen toimivaltuuksilla[64]. Kun toiminta tapahtuu normaaliolojen ja poikkeusolojen välimaastossa, puhutaan normaaliolojen häiriötilanteista[65].



Kuvio 1. Hybridiuhan käsite.

[62] HE 202/2017 vp, s. 10.
[63] Valtioneuvosto, 2021a, s. 17.
[64] HE 94/2022 vp, s. 4.
[65] HE 63/2022 vp, s. 7.

Hybridiuhat voidaan siis nähdä kansainvälisesti tunnistettuna kattoterminä useita keinoja hyödyntävälle hybridivaikuttamiselle ja -sodankäynnille. Kuitenkin termien merkitys saattaa hieman erota eri asiayhteyksissä, sillä poliittisessa, akateemisessa ja sotilaallisessa asiayhteydessä erilaiset toimet saattavat painottua enemmän[66]. Tässä tutkimuksessa hybridivaikuttamisesta puhuttaessa tarkoitetaan sitä toimintaa, joka muodostaa hybridiuhkan ja tämä toiminta voi olla myös hybridisodankäyntiä. Hybridiuhat ovat siis valtioon kohdistuvia uhkia, jotka konkretisoituvat toiminnaksi hybridivaikuttamisen tai hybridisodankäynnin kautta. Näin ollen hybridiuhat ovat monista eri keinoista koostuvia mahdollisia tapahtumakulkuja, jotka muuttuvat uhkasta todelliseksi toiminnaksi, kun näitä keinoja aletaan toteuttaa hybridivaikuttamisen tai -sodankäynnin avulla. Hybridiuhkien, hybridivaikuttamisen ja hybridisodankäynnin yhteyksiä ja käsitteitä on havainnollistettu kuviossa 1.

Vuoden 2023 kansallisessa riskiarviossa hybridivaikuttamista kuvataan vahingolliseksi toiminnaksi, joka voi pitää sisällään laillisia sekä laittomia keinoja, joita toteutetaan samanaikaisesti tai toistensa jatkumoina kohteen haavoittuvuuksiin vaikuttaen. Hybridivaikuttamista pyritään toteuttamaan niin, että toiminta on tekijän puolelta kiistettävissä, vaikka vaikuttaminen voikin kohdistua suoraan, mutta myös epäsuorasti, yhteiskunnan toimintoihin.[67] Tällainen epämääräinen toiminta, jonka tarkoitusperiä kohdevaltion on vaikea tulkita, vaikeuttaa operaation julkista syyksiluettavuutta eli attribuutiota jonkin toisen valtion tai ei-valtiollisen toimijan tekemäksi, koska kohdevaltion voi olla vaikea tunnistaa, ohjataanko operaatiota tietoisesti ja jos ohjataan, niin kenen toimesta[68]. Näin ollen hybridivaikuttamisen piiriin kuuluvan toiminnan selvittäminen oikeusteitse on usein lähes mahdotonta, koska toiminnan tekijää ja sillä saavutettuja seurauksia voi olla vaikea näyttää toteen. Riittävän näytön kerääminen operaation toteuttajaa vastaan on

[66] Giannopoulos, Smith & Theocharidou, 2021, s. 9–10.
[67] Sisäministeriö, 2023a, s. 24–25.
[68] Ferm, 2018, s. 407.

kuitenkin tärkeää tulevaisuuden kannalta, koska tehokas hyökkääjän nimeäminen eli attribuutio voi toimia ennaltaehkäisevänä pelotteena, vaikka tekijöitä ei saataisikaan vastuuseen toimista[69].

Voimankäytön oikeussäännöissä todetaan, että kansainvälisessä oikeudessa hybridiuhkat tai hybridisodankäynti eivät muodosta oikeussääntelyn ulkopuolelle jäävää ”harmaata aluetta” sodan ja rauhan välimaastoon[70]. Vaikuttamistoiminnan tunnistamista ja todentamista vaikeuttaa kuitenkin se, että hybridivaikuttamisen keinoja hyödynnetään eri viranomaisten vastuualueilla, jolloin niihin ei välttämättä voida vastata viranomaisten tavanomaisten toimivaltuuksien avulla tai toimia ei edes tunnisteta[71]. Tällöin eräänlainen ”harmaa alue” koostuu eri viranomaisten toimivaltuuksien rajapinnasta sekä sisäisen ja ulkoisen turvallisuuden rajasta, jolloin kohdevaltion viranomaisilla on epäselvät keinot puuttua toimintaan ja tätä epäselvyyttä tekijät hyödyntävät.

Ferm painottaakin, että toimivaltaisten viranomaisten toimivaltuuksia hybridiuhkiin vastaamiseksi tulee parantaa ja selkiyttää, ja huomiota tulee kiinnittää erityisesti toimivaltuuksien rajapintoihin ja epämääräisiin keinoihin, joilla puututaan valtion sisäisiin asioihin, mutta jotka eivät ylitä voimankäytön rajaa[72]. Myös puolustusvaliokunta on mietinnössään korostanut, että viranomaisyhteistyötä toteutettaessa toimivaltuuksien rajapinnassa ei saa olla aukkoja tai epäselvyyksiä, joita ulkopuoliset tahot voivat pyrkiä hyödyntämään[73]. Yhtenä hybridivaikuttamiseen varautumista ja vastaamista edistävänä keinona on esitetty osittain päällekkäisten viranomaistoimivaltuuksien säätämistä, jotta hybridiuhkiin, joissa viranomaisia kuormitetaan useilla samanaikaisilla tehtävillä, voidaan vastata ketterämmin[74]. Aine, Nurmi ja Valtonen esittävätkin, että kokonaisturvallisuutta toteuttavien toimijoiden toimivaltuuksista säätävän lainsäädännön tulee olla aiempaa

[69] Euroopan hybridiuhkien osaamiskeskus, 2022, s. 2.
[70] Voimankäytön oikeussäännöt, 2015, s. 36.
[71] Sisäministeriö, 2023a, s. 27.
[72] Ferm, 2018, s. 419.
[73] PuVM 2/2022 vp, s. 5.
[74] HE 201/2017 vp, s. 13.

eheämpi kokonaisuus, jossa lainsäädännön osa-alueet limittyvät toisiinsa, jotta varmistetaan toimivaltuuksien joustava käyttö erilaisissa tilanteissa[75].

2.1.1 Keinoja hybridiuhkien synnyttämiseksi

Hybridiuhkien määrittely perustuu yleensä niiden keinojen kuvailuun, joita hybridivaikuttamisessa tai -sodankäynnissä hyödynnetään[76]. Hybridiuhka muodostuu toiminnasta, jossa voidaan hyödyntää muun muassa taloudellisia, poliittisia, diplomaattisia, teknisiä tai sotilaallisia keinoja sekä informaatio- ja kybervaikuttamista. Osana hybridivaikuttamista voidaan esimerkiksi hankkia kiinteistöjä kohteena olevan valtion strategisilta alueilta ja pyrkiä näin heikentämään viranomaisten toimintaedellytyksiä tai muuten tukemaan vieraan valtion tavoitteita esimerkiksi edistämällä laitonta tiedustelutoimintaa[77].

Vaikuttamista voi tapahtua myös pandemioiden ja epidemioiden ohella sekä siinä voidaan hyödyntää muuttoliikettä, pakolaisia tai hybridivaikuttamista toteuttavien maiden kohdevaltiossa oleskelevia kansalaisia[78]. Euroopan komissio kuvaa tiedonannossaan hybridivaikuttamisessa hyödynnettävää muuttoliikettä muuttajien välineellistämisellä, jossa kolmannen maan toimija käyttää turvapaikanhakijoita tai laittomasti maahan pyrkiviä ihmisiä välineenä horjuttaakseen unionin tai sen jäsenvaltioiden vakautta ja yhtenäisyyttä ohjaamalla laittomia muuttovirtoja unionin ulkorajoille, joko omalta alueeltaan tai sen kautta[79]. Myös muuttoliikkeen välineellistämisen taustalla voi olla muu kuin valtiollinen toimija[80]. Tämänlaista operatiivista toimintaa on nähty viime aikoina muun muassa Valko-Venäjän rajalla vuonna 2021, jolloin muuttoliike kohdistui Puolaan, Latviaan

[75] Aine, Nurmi & Valtonen, 2022, s. 872.
[76] HaVM 10/2017 vp, s. 2.
[77] HE 258/2018 vp, s. 2.
[78] HaVL 30/2021 vp, s. 3; Sisäministeriö, 2022, s. 10.
[79] COM(2021) 891 final, s. 7 ja 35.
[80] HaVL 19/2022 vp, s. 9.

ja Liettuaan sekä Venäjän ja Suomen välisellä rajalla syksystä 2023 lähtien maahantulon kohdistuessa Suomeen[81].

Keskeisenä hybridivaikuttamisen ja hybridisodankäynnin keinona esiin nousee informaatiovaikuttaminen, jonka tavoitteena on häiritä yhteiskuntarauhaa ja ohjata päätöksentekoa esimerkiksi levittämällä disinformaatiota, jakamalla vaillinaista tietoa tai jopa jättää olennaista tietoa jakamatta[82]. Björn ja Puistola huomauttavat, että informaatiovaikuttamisen osana voidaan hyödyntää myös vaalivaikuttamista, jossa pyritään kärjistämään ristiriitoja, viljelemään salaliittoteorioita, leimaamaan ja maalittamaan poliittisia päätöksentekijöitä, kiistämään vaalitulosta horjuttaen järjestelmän luotettavuutta sekä hyödyntämään erilaisia trolleja ja botteja sosiaalisessa mediassa. Näiden keinojen avulla pyritään vaikuttamaan äänestäjiin, mikä voi auttaa esimerkiksi vaikuttajavaltiota pääsemään poliittisiin päämääriinsä, mutta myös puolueita markkinoimaan päämäärinsä, jolloin jälkimmäinen toiminta ei liity hybridivaikuttamiseen.[83]

Hybridivaikuttamista onkin vaikea tunnistaa juuri siksi, että toiminta voi olla tavanomaista toimintaa, jonka luonteen selvittäminen hybridivaikuttamiseksi vaatii toiminnan taustalla olevan tahon ja sen tavoitteiden selvittämistä. Esimerkiksi jokin salaliittoteoria itsessään ei lähtökohtaisesti ole hybridivaikuttamista, mutta jos salaliittoteoria on kehitetty vaikkapa avuksi propagandan levittämiseen, jolloin Räikän mukaan salaliittoteorian tavoitteena on usein mustamaalata jotakin maata, voi kyseessä olla toisen valtion tavoitteellinen toiminta heikentää mustamaalattavan valtion poliittista asemaa niin sisäisesti kuin kansainvälisessä yhteisössäkin. Lisäksi Räikän mukaan salaliittoteorioita voidaan ke-

[81] Kuvatun operatiivisen toiminnan johdosta hallitus asetti 19.2.2024 säädöshankkeen maahantulon välineellistämisen torjumiseksi ja rajaturvallisuuden vahvistamiseksi (SM004:00/2024). Hankkeen pohjalta hallitus antoi 15.3.2024 luonnoksen hallituksen esitykseksi eduskunnalle laiksi väliaikaisista toimenpiteistä välineellistetyn maahantulon torjumiseksi. Esityksen tavoitteena on tehokkaasti torjua maahantulon välineellistämisen muodossa Suomeen kohdistettavaa painostamista, vahvistaa rajaturvallisuutta ja varautua välineellistetyn maahantulon vakavimpiin tilanteisiin. Esitys toteuttaa hallitusohjelman tavoitetta muun muassa ennakoivasta hybridiuhkiin varautumisesta. (HE-luonnos, 15.3.2024, s. 1) Hankkeen pohjalta pyritään antamaan varsinainen hallituksen esitys huhtikuussa 2024.
[82] HaVM 19/2021 vp, s. 14.
[83] Björn & Puistola, 2023, s. 80.

hittää muun muassa poliittisen päätöksenteon hankaloittamiseksi, jolloin hybridivaikuttaja voi strategisesti pyrkiä kylvämään kohdemaan keskuudessa esimerkiksi kiistanalaisia asiantuntijalausuntoja, huhuja ja disinformaatiota.[84] Salaliittoteorioiden levittäminen ei lähtökohtaisesti ole hybridivaikuttamista, mutta niitä voidaan luoda hybridivaikuttamisen tehostamiseksi, jolloin on tärkeää pyrkiä selvittämään salaliittoteorian kehittäjä ja sen tavoitteet.

Valtioneuvoston kanslian keskustelupaperissa todetaan, että erityisesti informaatiovaikuttamisessa, mutta myös kaikilla hybridivaikuttamisen osa-alueilla, hyödynnetään usein psykologisia taustavaikuttimia, joilla pyritään tehostamaan esimerkiksi informaation sosiaalisia ja emotionaalisia vaikutuksia kohdeyleisössä. Keskustelupaperissa tällaisesta toiminnasta käytetään termiä kognitiivinen intruusio, jolla kuvataan sosiaalisia ja psykologisia painostus- ja tehokeinoja sisältävää tehokasta mekanismia, jolla pyritään vaikuttamaan ihmisten ja yhteisöjen asenteisiin ja käyttäytymiseen. Kun kognitiivisen intruusio on onnistunutta ja tehokasta, se edesauttaa hybridivaikuttamisen tavoitteiden saavuttamista.[85]

Informaatiovaikuttamiseen usein kytkeytyvä kybervaikuttaminen voi esiintyä esimerkiksi palvelunestohyökkäyksinä, erilaisten vakoiluohjelmien hyödyntämisenä tai sähköverkon häirintänä, jolloin pyritään hyökkäämään valtion kriittiseen infrastruktuuriin[86]. Kybervaikuttamisella voidaan pyrkiä vaarantamaan yhteiskunnan elintärkeitä toimintoja tai muita toimintoja, jotka ovat riippuvaisia kybertoimintaympäristöstä taikka vaarantamaan tietoturvan toteutumista, jolloin tiedon saatavuus, eheys ja luottamuksellisuus vaarantuvat[87].

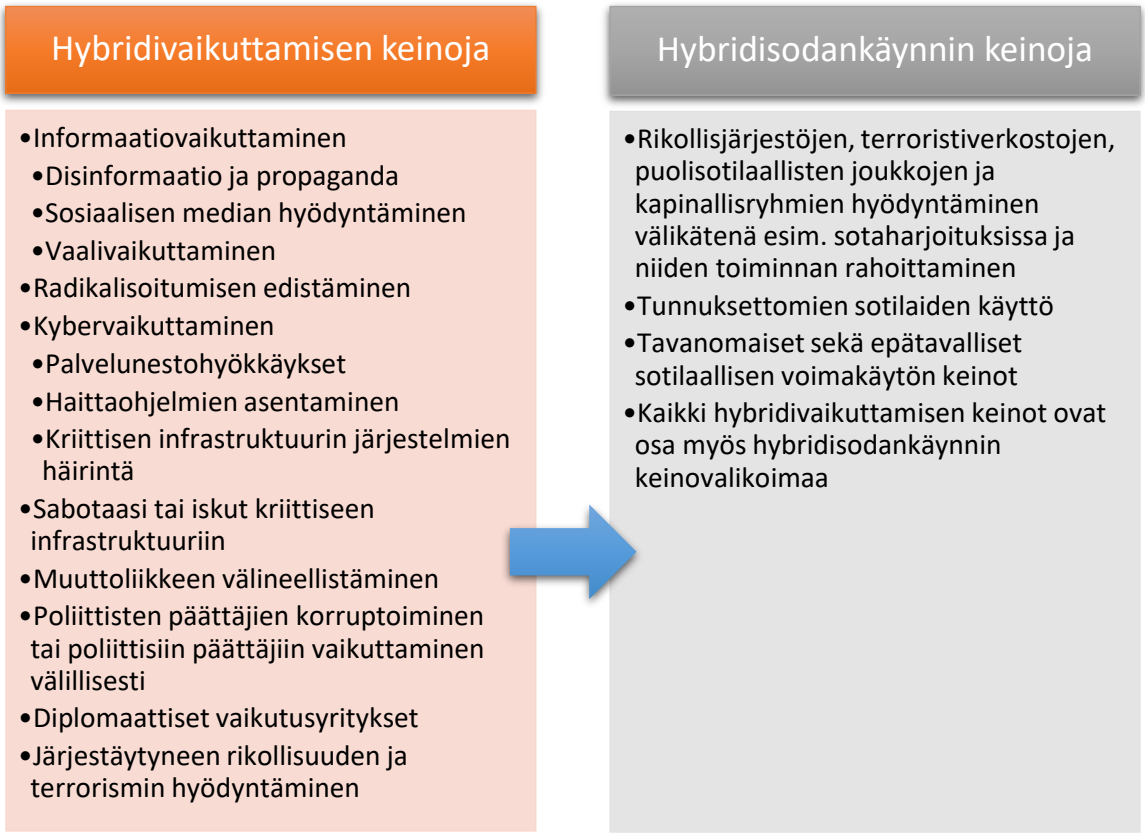
[84] Räikkä, 2021, s. 98–101.
[85] Valtioneuvoston kanslia, 2023, s. 8.
[86] Valtioneuvosto, 2022, s. 8.
[87] Kokonaisturvallisuuden sanasto, 2017, s. 34.

Hybridivaikuttamisen keinoja voivat siis olla kyberoperaatiot, väärän tiedon ja propagandan levittäminen sekä vaikuttaja-agenttien värväämineni, poliittisten ääriliikkeiden rahoittaminen tai jopa poliittisten päättäjien korruptoiminen[88]. Osa toimista on aineettomia toimia, kuten useimmat informaatiovaikuttamisen keinot ja diplomaattiset vaikutusyritykset, mutta hybridivaikuttamisessa voi esiintyä myös fyysisiä eli aineellisia toimia, kuten iskut valtion kriittiseen infrastruktuuriin tai sotilaallisen voimankäytön keinot[89]. Toimet voivat olla laitonta valtion sisäisiin asioihin puuttumista, jos niillä pyritään painostamaan valtiota sen oman harkintavallan piiriin kuuluvissa asioissa tai vaikkapa lietsomaan väestön sisäisiä ristiriitoja[90]. Myös lailliset keinot voivat olla osa hybridivaikuttamisen toimintakenttää, jolloin laillisia keinoja hyödynnetään tekijän omiin tavoitteisiin pääsemiseksi. Esimerkiksi ulkomaalaiset yritysostot tai aiemmin mainitut kiinteistöhankinnat voivat mahdollistaa valtiollisen vaikuttamistoimijan pääsyn kohdemaan kriittiseen infrastruktuuriin, jolloin sen turvaaminen vaikeutuu[91]. Kun edellä mainittuja laittomia ja laillisia keinoja toteutetaan yhdessä onnistuneesti, on kohdevaltion haastavaa havaita toimia sekä niiden synnyttämää uhkaa ja ryhtyä vaadittaviin vastatoimiin[92].

Nämä esitetyt keinot ovat kuitenkin vain esimerkkejä jo tunnistetuista hybridivaikuttamisen keinoista, minkä vuoksi on tärkeää tiedostaa, että hybridiuhkia tavoitteleva toimija pyrkii keksimään koko ajan uusia keinoja tavoitteidensa saavuttamiseksi. Näin ollen niin keinot kuin hybridiuhkan määritelmäkin on haluttu jättää niin kansainvälisessä kuin kansallisessakin keskustelussa joustavaksi, jotta toiminnan muuttuva luonne pystytään huomioimaan toiminnan tunnistamisessa[93]. Kuvioon 2 on tiivistetty erilaisia jo tunnistettuja keinoja, joita hybridivaikuttamisessa ja hybridisodankäynnissä voidaan hyödyntää. Kuviota tarkastellessa on tärkeää muistaa, että hybridisodankäynnissä voidaan hyödyntää kaikkia hybridivaikuttamisen keinoja osana sotilaallista voimankäyttöä, joten hybridivaikuttamisen keinot soveltuvat myös hybridisodankäyntiin.

---

[88] Mikkola ja muut, 2018, s. 26.
[89] Sisäministeriö, 2023a, s. 27.
[90] Voimankäytön oikeussäännöt, 2015, s. 40.
[91] UaVM 5/2022 vp, s. 17.
[92] Mikkola ja muut, 2018, s. 26.
[93] HaVM 10/2017 vp, s. 2.



Kuvio 2. Hybridivaikuttamisen ja hybridisodankäynnin erilaisia keinoja.

Vaikka hybridivaikuttamisessa ja hybridisodankäynnissä hyödynnetään monenlaisia keinoja, on tärkeää muistaa, että kaikki onnettomuudet ja häiriöt esimerkiksi sähkö- tai tietoverkoissa eivät ole hybridivaikuttamista. Hybridivaikuttamisen takana voi olla monenlaisia toimijoita, ja vaikka toimija tunnistettaisiinkin, voi kyseessä olla hybridivaikuttamisesta täysin irrallinen vahingonteko. Tämä osaltaan vaikeuttaa hybridiuhkien ja hybridivaikuttamisen tunnistamista, koska erilliseltä vaikuttava teko voi olla osa organisoitua vaikuttamistoimintaa tai pelkkää sattumaa. Tämän vuoksi viranomaisten yhteinen tilannekuva, viranomaisten välinen tietojenvaihto ja kokonaisturvallisuuden toimintamallin toteuttaminen ovat keskeisessä roolissa hybridiuhkien tunnistamisessa ja niiden torjumisessa[94].

[94] HaVM 19/2021 vp. s. 12.

2.1.2 Uhkia aiheuttavat toimijat ja uhkatoimien oikeudellinen arviointi

Hybridiuhkien taustalla oleviksi toimijoiksi mielletään usein valtiolliset toimijat ja valtiosta riippumattomat ryhmittymät, mutta myös yksittäiset henkilöt tai henkilöryhmät voivat olla toiminnan takana[95]. Hybridiuhkat kohdistuvat demokraattisiin valtioihin, jolloin valtiolliset toimijat ovat usein autoritaarisia valtioita, jotka pyrkivät hybriditoiminnallaan horjuttamaan ja heikentämään demokraattisten valtioiden voimavaroja samalla parantaen omia strategisia intressejään[96]. Se, että autoritaarisen valtion johtaja näkee länsimaat ja demokratian omalle toiminnalleen uhkana ei ole itsessään länsimaita uhkaava hybridiuhka, sillä autoritaarinen valtio voi hyödyntää strategisia tavoitteitaan saavuttaakseen perinteisiä läpinäkyviä vaikuttamiskeinoja, kuten ulkopolitiikkaa, diplomatiaa ja oikeudellisia sopimuksia[97]. Hybridiuhka muodostuu sen sijaan silloin, kun valtiollisella toimijalla ei ole kykyjä edistää strategisia etujaan perinteisiä keinoja käyttäen, vaan se ryhtyy toteuttamaan monia eri keinoja hyödyntäviä hybriditoimia demokraattista valtiota vastaan tavoitteidensa saavuttamiseksi[98].

Valtiolliset toimijat voivat hyödyntää toiminnassaan välikätenä myös kapinnallisryhmiä, rikollisjärjestöjä tai tunnuksettomia sotilaita, jollaisia Venäjä on esimerkiksi hyödyntänyt sotaharjoituksissaan Ukrainassa ja Syyriassa[99]. Kuitenkin ylikansalliset järjestäytyneet rikollisryhmät ja terroristiverkostot voivat yksinäänkin pyrkiä vaikuttamaan valtioihin ja kohdeyleisöönsä esimerkiksi sosiaalisen median kautta jossain määrin hybridivaikuttamisen tavoin, mutta harvoilla tällaisista ryhmittymistä on kapasiteettia ja kykyjä yksinään toteuttaa strategisia ja koordinoituja hybridioperaatioita länsimaihin, vaan useimmiten

[95] HaVM 19/2021 vp, s. 12.
[96] Giannopoulos, Smith & Theocharidou, 2021, s. 16.
[97] Giannopoulos, Smith & Theocharidou, 2021, s. 15.
[98] Giannopoulos, Smith & Theocharidou, 2021, s. 15–16.
[99] Sadik, 2022, s. 4; HE 63/2022 vp, s. 52.

ne toimivat valtiollisten toimijoiden kanssa yhteistyössä[100]. Terroristijärjestöjen ja -verkostojen etu on kuitenkin niiden kyvykkyys muuttaa muotoaan ja hyödyntää rajat ylittävän rikollisuuden muotoja sekä uutta teknologiaa osana terroritekoa, mutta myös osana ihmisten värväämistä[101]. Ei-valtiollisten ryhmittymien rooli on siis tärkeää tiedostaa hybridiuhkien tunnistamiseksi, jotta sellaistenkin toimijoiden toimet voidaan tarvittaessa tunnistaa osaksi hybridivaikuttamista tai hybridisodankäyntiä.

Giannopoulos, Smith ja Theocharidou esittävät, että hybridiuhkien kontekstissa valtioista riippumattomat toimijat ovat usein ryhmittymiä, jotka osallistuvat kansainvälisiin suhteisiin ja joilla on riittävästi valtaa puuttua, vaikuttaa ja aiheuttaa muutoksia ilman mitään sidonnaisuutta vakiintuneisiin valtion instituutioihin. Ne vaikuttavat häirinnän avulla usein hitaasti ja hienovaraisesti ja voivat näin jopa haastaa kansallisvaltiot ja painostaa demokraattisia hallituksia.[102] Hybridiuhkien mekanismeja hyödyntävistä valtiosta riippumattomista toimijoista puhuttaessa on viitattu esimerkiksi erilaisiin terroristijärjestöihin, useisiin välillisiin toimijoihin, kansainvälisiin järjestäytyneen rikollisuuden ryhmiin, ideologisiin liikkeisiin sekä voittoa tavoitteleviin ”freelance”-toimijoihin, jotka hyödyntävät hybriditoimintaa tehostaakseen toimintatapoja, jotka edistävät heidän strategisia intressejään[103]. Valtiosta riippumattomat toimijat hyödyntävät usein toiminnassaan moderneja sotilaallisia voimavaroja kuten pienikokoisia kauko-ohjattavia ohjuksia ja salattuja komentojärjestelmiä, joiden avulla ne pyrkivät iskemään länsimaisten armeijoiden haavoittuvuuksiin[104]. Voi siis olla, että valtiosta riippumattomat toimijat hyödyntävät hybridivaikuttamisen keinoja useimmiten osana hybridisodankäyntiä.

Hybridisodankäynnin ja hybridivaikuttamisen osatekijöitä voidaan arvioida oikeudellisesti, vaikka ne eivät ole oikeudellisia käsitteitä eikä niistä ole valtiollista oikeuskäytäntöä tai valtiokäytäntöä[105]. Hybridivaikuttamiseen sisältyy monenlaisia toimintamuotoja,

[100] Giannopoulos, Smith & Theocharidou, 2021, s. 24–25.
[101] Lohse, Meriniemi ja Honkanen, 2019, s. 30–31.
[102] Giannopuolos, Smith & Theocharidou, 2021, s. 22.
[103] Giannopoulos, Smith & Theocharidou, 2021, s. 16.
[104] Hoffman, 2009, s. 5.
[105] Voimankäytön oikeussäännöt, 2015, s. 39.

joista vain osa kuuluu tai on rinnastettavissa valtioiden välisen aseellisen voimankäytön piiriin[106]. Hybridivaikuttamisessa ja -sodankäynnissä pyritään toimimaan alueella, joka ei täytä rikosoikeudellisten toimien piirteitä eikä myöskään sodankäynnin kynnystä. Voimankäytön oikeussääntöjen mukaan YK:n peruskirjan (SopS 1/1956) kielletyn voimankäytön kynnys ylittyy kuitenkin viimeistään siinä kohtaa, kun toisen valtion alueella toteutetaan aseellisia operaatioita ilman valtion suostumusta, joko hyökkääjävaltion omien asevoimien tai sen käyttämien välillisten asevoimien toimesta. Jos aseellisen voimankäytön kynnys ei ylity, voidaan hybridiuhkia arvioida esimerkiksi tapaoikeudellisen YK:n peruskirjan toisen valtion sisäisiin asioihin puuttumisen kiellon näkökulmasta ja mikäli toiminta ei kuulu kansainvälisen oikeuden piiriin, se voi kuulua kansallisen rikosoikeudellisen toimivallan piiriin.[107] Esimerkiksi kybervaikuttamisen tai kriittiseen infrastruktuuriin kohdistetuissa iskuissa voi tulla kyseeseen jokin rikoslain (39/1889) 35 luvun 1–3 §:ssä mainituista vahingonteon muodoista sisältäen myös 3 a-c §:ssä mainitut datavahingonteot taikka jokin 38 luvun 5–8 b §:ssä mainituista rikoksista.

Useimmiten terroristi- ja rikollisjärjestöjen käyttämät hybridivaikuttamisen keinot kuuluvat rikosoikeudellisen sääntelyn piiriin, sillä toimia ohjataan usein kohteena olevan valtion alueelta. Jos taas tällaistakin toimintaa on johdettu tai toteutettu toisesta valtiosta käsin, voi kyseeseen tulla kansainvälisen oikeuden vastuukysymykset kohdevaltion mahdollisesta myötävaikutuksesta tai laiminlyönnistä.[108] Jotta erityisesti valtiollisten toimijoiden synnyttämien hybridiuhkien havaitsemista ja niiden ennakollista torjumista voitaisiin parantaa, tulee EU:lla ja jäsenvaltioilla olla riittävät toimivaltuudet vastatiedusteluun niin siviili- ja sotilastiedustelun alaan kuuluvissa asioissa[109]. Seuraavaksi tarkastelenkin, miten nykyiset kansalliset tiedustelutoimivaltuudet vastaavat hybridiuhkien haasteisiin ja ovatko toimivaltuudet riittäviä.

---

[106] Voimankäytön oikeussäännöt, 2015, s. 36.
[107] Voimankäytön oikeussäännöt, 2015, s. 39.
[108] Voimankäytön oikeussäännöt, 2015, s. 39.
[109] Euroopan komissio, 2018, s. 5.

2.2 Tiedusteluviranomaiset ja tiedustelulainsäädännön mukaiset toimivaltuudet

Suomessa tuli 1. kesäkuuta 2019 voimaan uusi tiedustelulainsäädäntökokonaisuus, joka kattaa säännökset siviili- ja sotilastiedustelusta. Tätä ennen Suomessa ei ollut säädetty tiedustelutoiminnan keinoista tai siitä, mihin toiminnalla pyritään, joten tiedustelutoimivaltuudet koettiin puutteellisiksi ja lainsäädäntökokonaisuutta alettiin valmistelemaan[110]. Siviilitiedustelua koskevat säännökset sisältyvät poliisilain (872/2011, siviilitiedustelua koskeva 5 a luku saatettu voimaan lailla 581/2019) 5 a lukuun sekä erilliseen säädökseen tietoliikennetiedustelusta siviilitiedustelussa (582/2019). Sotilastiedustelusta sen sijaan säädetään laissa sotilastiedustelusta (590/2019). Lainsäädäntökokonaisuuden antaminen mahdollistettiin säätämällä uusi laki tiedustelutoiminnan valvonnasta (121/2019) sekä lisäämällä luottamuksellisen viestinnän suojaa koskeva perustuslain 10 §:n 4 momentti, jonka mukaan viestin salaisuuteen voidaan lailla säätää välttämättömiä rajoituksia muun muassa tiedon hankkimiseksi sotilaallisesta toiminnasta tai muusta vakavasti kansallista turvallisuutta uhkaavasta toiminnasta[111].

Tiedustelulainsäädännön päätavoitteena on turvata paremmin kansalliseen turvallisuuteen kohdistuvia uhkia ja viimeisimmän ulko- ja turvallisuuspoliittisen selonteon mukaan lainsäädäntö mahdollistaakin kansalliseen turvallisuuteen ja maanpuolustukseen kohdistuvien uhkien tehokkaamman havaitsemisen[112]. Tiedonhankintalakityöryhmän mietinnössä tiedustelulakien tavoitteeksi asetettiin ylimmän valtionjohdon sekä turvallisuusviranomaisten tiedonsaannin parantaminen näistä uhista ja Suomen turvallisuusympäristön kehittymisestä[113].

[110] Puolustusministeriö, 2015, s. 14.
[111] Valtioneuvosto, 2021b, s. 7.
[112] Valtioneuvosto, 2020, s. 34.
[113] Puolustusministeriö, 2015, s. 13–14.

Turvallisuusviranomaisia ovat kaikki kansalliset sisäisen ja ulkoisen turvallisuuden toimijat, joiden lakisääteisiin tehtäviin kuuluu turvallisuuden ylläpitäminen[114]. Turvallisuusviranomaisiksi katsotaan myös tiedustelulakien myötä määritetyt tiedusteluviranomaiset, jotka ovat tämän tutkielman keskiössä. Tiedonhankintatyöryhmän mietinnössä tiedonhankintaa suorittaviksi toimivaltaisiksi turvallisuusviranomaisiksi eriteltiin suojelupoliisi ja Puolustusvoimat, joiden tehtävänä on ollut kansalliseen turvallisuuteen kohdistuvien uhkien torjunta jo ennen nykyisiä tiedustelulakeja[115]. Siispä olikin luontevaa lähteä muovaamaan tiedustelulakeja näiden viranomaisten toimivaltuuksiin keskittyen, joten tiedustelulakien mukaisesti suojelupoliisin toimivaltaan kuuluu siviilitiedustelun suorittaminen (PolL 5a:1), kun taas sotilastiedustelua toteuttaa Puolustusvoimat (SotTiedL 1 §).

2.2.1 Tiedustelun tarkoitus

Poliisilain 5 a luvun 1 §:n mukaan siviilitiedustelun tarkoituksena on tiedon hankkiminen ja sen hyödyntäminen kansallisen turvallisuuden suojaamiseksi sekä hankitun tiedon toimittaminen ylimmälle valtionjohdolle tai muille viranomaisille kansalliseen turvallisuuteen liittyvien tehtävien suorittamiseksi. Suojelupoliisi voi käyttää tiedustelumenetelmin hankkimaansa tietoa itse kansallisen turvallisuuden suojaamiseksi, tai jakaa tiedon muille asiaan kuuluville viranomaisille, joilla on kansallisen turvallisuuden suojaamiseen kuuluvia tai siihen liittyviä tehtäviä, ja velvollisuus auttaa näiden tehtävien hoitamisessa[116]. Näin varmistetaan tiedonhankinnan käyttötarkoitussidonnaisuus eli että siviilitiedustelulla hankittua tietoa hyödynnetään nimenomaan kansallisen turvallisuuden suojaamiseksi[117]. Näin ollen siviilitiedustelutoiminnalla saatu tieto voi mahdollistaa muiden turvallisuusviranomaisten ennakollisen ryhtymisen kansallista turvallisuutta uhkaavien toimien torjuntaan ja sillä varmistetaan valtionjohdon päätöksenteon perustuminen luotettavaan ja ajantasaiseen tietoon[118].

---

[114] Sisäisen turvallisuuden sanasto, 2023, s. 11.
[115] Puolustusministeriö, 2015, s. 48.
[116] HE 202/2017 vp, s. 169.
[117] HE 202/2017 vp, s. 169.
[118] HE 202/2017 vp, s. 169.

Tässä vaiheessa on hyvä tehdä ero suojelupoliisin suorittaman siviilitiedustelun ja poliisin toimivaltaan kuuluvien salaisten tiedonhankintakeinojen välille. Poliisilain 5 luku sisältää säännökset poliisin toimivallasta käyttää salaisia tiedonhankintakeinoja, kuten esimerkiksi telekuuntelua tai peiteltyä tiedonhankintaa, rikosten estämiseen, paljastamiseen tai vaaran torjumiseen. PolL 5 luvun 2 §:n 1 momentissa todetaan, että salaisen tiedonhankintakeinon käytön edellytyksenä on, että sen avulla voidaan olettaa saatavan tarvittavia tietoja, joiden avulla voidaan estää tai torjua jokin rikos tai vaara. Näin ollen poliisin salaiset tiedonhankintakeinot liittyvät nimenomaan rikosten torjumiseen tai estämiseen, kun taas suojelupoliisin tiedustelutoimivaltuudet koskevat PolL 5a luvun 1 §:n mukaan tiedonhankintaa ja tiedon hyödyntämistä kansallisen turvallisuuden suojaamiseksi, ylimmän valtionjohdon päätöksenteon tukemiseksi ja muiden turvallisuusviranomaisten lakisääteisien tehtävien suorittamiseksi. Kuitenkin lakiin on jätetty erityissäännös tilanteista, joissa siviilitiedustelun aikana havaitaan, että henkilön oletetaan perustellusti syyllistyvän tai syyllistyneen PolL 5 luvun 3 §:ssä mainittuihin rikoksiin, jolloin suojelupoliisi saa jatkaa tiedustelumenetelmän käyttöä salaisena tiedonhankintana korkeintaan kuukauden rikosten paljastamiseksi tai estämiseksi (PolL 5a:5). Tiedustelumenetelmien ja salaisten tiedonhankintakeinojen erona toimii siis menetelmien käyttötarkoitus, eli käytetäänkö menetelmiä kansallisen turvallisuuden suojaamiseksi vai rikosten paljastamiseksi tai estämiseksi.

Siviilitiedustelussa voidaan hyödyntää samoja menetelmiä kuin poliisin suorittamassa salaisessa tiedonhankinnassa, jolloin tiedustelumenetelmien käytön edellytykset eroavat salaisten tiedonhankintakeinojen edellytyksistä siten, että suojelupoliisin tiedustelumenetelmillä hankitaan tietoa kansallisen turvallisuuden takaamiseksi, kun taas poliisin salaisilla tiedonhankintakeinoilla hankitaan tietoa rikosten estämiseksi ja torjumiseksi[119]. Näiden lisäksi sallittuja tiedustelumenetelmiä ovat PolL 5a luvun 2 §:ssä luetellut paikkatiedustelu, jäljentäminen ja lähetyksen jäljentäminen sekä lähetyksen pysäyttäminen jäljentämistä varten. Siviilitiedustelussa voidaan hyödyntää myös tietoliikennetiedustelua,

[119] HE 202/2017 vp, s. 72.

josta säädetään erikseen laissa tietoliikennetiedustelusta siviilitiedustelussa. TtStL 2.1 §:n 1 kohdassa tietoliikennetiedustelulla tarkoitetaan viestintäverkossa Suomen rajan ylittävään tietoliikenteeseen kohdistuvaa teknistä tiedonhankintaa, joka toteutetaan tietoliikenteen automatisoidun erottelun avulla sekä näin hankitun tiedon käsittelyä.

Sotilastiedustelussa sen sijaan on kyse tiedon hankkimisesta Suomeen kohdistuvista ulkoisista uhkista sekä ylimmän valtionjohdon päätöksenteon tukeminen erityisesti pitämällä ylin valtionjohdon tietoisena turvallisuusympäristössä tapahtuvista muutoksista[120]. SotTiedL 3 §:n mukaan sotilastiedustelulla hankitaan ja käsitellään tietoa Suomeen kohdistuvasta tai Suomen turvallisuusympäristön kannalta oleellisesta sotilaallisesta toiminnasta taikka 4 §:n 2 momentissa tarkoitetusta toiminnasta erityisesti ylimmän valtionjohdon päätöksenteon tueksi ja säännöksessä lueteltujen tiettyjen Puolustusvoimien lakisääteisten tehtävien suorittamiseksi. SotTiedL 4 § 2 momentin mukaan sotilastiedustelulla hankitaan tietoa myös vieraan valtion toiminnasta tai muusta sellaisesta toiminnasta, joka vakavasti uhkaa Suomen maanpuolustusta tai vaarantaa yhteiskunnan elintärkeitä toimintoja. Näin ollen sotilastiedustelun tarkoitus pohjautuu Puolustusvoimista annetun lain mukaisiin lakisääteisiin tehtäviin ja sen tarkoituksena on tuottaa myös oikeaa ja riippumatonta tietoa ennakoivasti ylimmän sotilasjohdon ja lopulta ylimmän valtionjohdon päätöksenteon tueksi[121].

Sotilastiedustelussa on siis kysymys sotilaallisen toiminnan tai muun Suomen maanpuolustusta tai kriittisiä toimintoja uhkaavan toiminnan havaitsemisesta tiedonhankinnan avulla. Laissa tarkoitettu sotilaallinen toiminta voi olla sekä valtiollista että ei-valtiollista toimintaa[122]. Tämä tarkoittaa, että sotilastiedustelu kattaa myös hybridisodankäyntiin- ja vaikuttamiseen liittyvän toiminnan. Tällöin sotilastiedustelulla pyritään hankkimaan tietoa toiminnan taustalla olevista tarkoitusperistä ja vaikuttimista sekä siitä, onko kyseessä

[120] HE 203/2017 vp, s. 178–179.
[121] HE 203/2017 vp, s. 179–180.
[122] OMML 41/2016, s. 48.

mahdollisesti vieraan valtion toimet, joiden jatkumona pyritään sotilaalliseen voimankäyttöön kohdevaltiota vastaan[123].

Myös sotilastiedustelussa hyödynnettävät tiedustelumenetelmät ovat samansuuntaisia kuin poliisin ja Puolustusvoimien jo ennen tiedustelulakeja olemassa olleet tiedonhankintakeinot rikosten estämiseksi ja torjumiseksi. Tällaisia keinoja ovat PolL 5 luvussa esitetyt salaiset tiedonhankintakeinot sekä sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain (255/2014, myöhemmin SKRTL) 9 luvun 89 §:ssä eritellyt toimivaltuudet. Koska sotilastiedustelussa ei ole kyse rikosten ennalta estämisestä tai torjumisesta, säädetään sotilastiedustelussa hyödynnettävistä menetelmistä erikseen SotTiedL 4 luvussa, joiden lisäksi sotilastiedusteluviranomaisella on käytössään sellaisia tiedonhankinnan keinoja, joiden käyttämiseen ei tarvita toimivaltuussääntelyä. Nämä tiedonhankinnan keinot ovat avointen lähteiden tiedustelu, kuvaustiedustelu ja geotiedustelu.[124] Kuten aiemmin on todettu, tiedustelutoimivaltuuksissa on kyse tiedon hankkimisesta sotilaallisesta toiminnasta ja ulkoisista uhkista, mistä sotilastiedustelulaki säätää, mutta Puolustusvoimilla on edelleen poliisilain 5 luvun ja sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain 9 luvun mukaiset toimivaltuudet käytössään rikosten torjumiseksi ja estämiseksi, jolloin toimivaltuudet määräytyvät niiden käyttötarkoituksen mukaan.

2.2.2 Tiedustelumenetelmät

Tiedusteluun kuuluu monenlaisia, toisiaan tukevia tiedustelumenetelmiä, joita yhdessä hyödyntämällä voidaan saada tietoa kansallisen turvallisuuden kannalta merkityksellisestä toiminnasta. Tiedustelutoiminnalla pyritään tunnistamaan kansallista turvallisuutta uhkaava toiminta sekä sen takana olevat henkilöt ja tahot, kuten valtiolliset ja

[123] HE 203/2017 vp, s. 181.
[124] HE 203/2017 vp, s. 218.

sotilaalliset toimijat[125]. Tiedustelulainsäädäntöryhmä nosti esiin kolme kansallisen turvallisuuden kannalta merkityksellisintä menetelmää, jotka ovat tietoliikennetiedustelu, ulkomaan henkilötiedustelu ja ulkomaan tietojärjestelmätiedustelu[126]. Tietoliikennetiedustelulla pyritään havaitsemaan ennakollisesti kansalliseen turvallisuuteen kohdistuvia uhkia, kun taas henkilötiedustelulla ja tietojärjestelmätiedustelulla hankitaan tietoa jo tunnistetuista uhkista[127]. Tietoliikennetiedustelun ja ulkomaan tiedustelun avulla pyritään hankkimaan tietoa myös mahdollisista kansainvälisistä uhkista[128].

Tiedustelulaeilla on säädetty suojelupoliisille ja Puolustusvoimille toimivaltuudet niin tietoliikennetiedusteluun kuin ulkomaan henkilötiedusteluun ja tietojärjestelmätiedusteluun[129]. Merkittävä muutos toimivaltuuksiin tuli tiedustelulakien myötä myös siltä osin, että ulkomaan tiedustelussa käytettyjä henkilötiedustelun ja tietojärjestelmätiedustelun menetelmiä voidaan nyt soveltaa myös kotimaan tiedustelussa ja siten Suomen rajojen sisäpuolella. Siviilitiedustelulain esitöissä menetelmien käytön mahdollistaminen esitettiin tarpeelliseksi, sillä kansallista turvallisuutta uhkaavaa toimintaa voidaan suunnitella myös Suomen alueella ja tällaisesta toiminnasta tiedon saaminen ajoissa mahdollistaa paremmin toiminnan etenemisen estämisen[130].

Laki tietoliikennetiedustelusta säätää suojelupoliisin toimivaltuuksista tietoliikennetiedustelussa ja SotTiedL 65–74 § säätävät sotilastiedustelussa hyödynnettävästä tietoliikennetiedustelusta. Tietoliikennetiedustelussa viranomainen hankkii kansallisen turvallisuuden kannalta merkittävää tietoa tietoliikenteestä ja sen sisällöstä[131]. TtStL 1 §:n ja SotTiedL 65 §:n mukaan tiedonhankinta tietoliikenteestä ei saa kuitenkaan olla kohdentamatonta ja yleistä tietoliikenteeseen kohdistuvaa seurantaa, vaan esimerkiksi TtStL 5 §:n mukaan tietoliikennetiedustelu kohdennetaan tietoliikenteeseen automatisoidun

[125] Valtioneuvosto, 2021b, s. 15.
[126] Puolustusministeriö, 2015, s. 50.
[127] HE 202/2017 vp, s. 109.
[128] HE 202/2017 vp, s. 113.
[129] HE 202/2017vp, s. 8; HE 203/2017 vp, s. 1
[130] HE 202/2017 vp, s. 72.
[131] Puolustusministeriö, 2015, s. 50.

erottelun avulla, joka perustuu hyväksyttyjen hakuehtojen käyttöön. Kyseessä voisi olla esimerkiksi luvan mukainen viestintäverkon osa, josta ohjataan tietoliikennettä tiedustelun suorittajalle, jolla on oikeus kerätä tietoliikenteestä hakuehtojen mukaisia viestejä[132]. Hallintovaliokunta on esittänyt, että hakuehdon hyväksyttävyyden perusteena tulee olla mahdollisimman tarkasti valittu tiedustelun kohteena oleva tietoliikenne, jotta puuttuminen luottamuksellisen viestin salaisuuden suojaan rajautuu tiedustelutehtävän kannalta välttämättömään[133].

Hakuehtona ei kuitenkaan saa käyttää Suomessa oleskelevan henkilön hallussa olevan tai tämän oletettavasti käyttävän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja (SotTiedL 68 § ja 70 §, TtStL 5.2 §). Lisäksi tietoliikennetiedustelun käytön edellytyksenä tulee olla tarpeellisuus tai välttämättömyys tärkeiden tietojen saamiseksi kansallisen turvallisuuden suojaamiseksi (TtStL 4 §) tai muuten kyseisen tiedustelutehtävän kannalta (SotTiedL 12 §). EIT on pohtinut välttämättömyyden vaatimusta erityisesti henkilöihin kohdistettavan tietoliikennetiedustelun tai henkilöihin kohdistettavien muiden salaisten tiedonhankintakeinojen osalta. EIT on jo tapauksessa Klass ja muut v. Saksa (6.9.1978) katsonut, että kansallisilla lainsäätäjillä on laaja, muttei rajoittamaton, harkintamarginaali välttämättömyyden arvioinnissa, kun salaisten tiedonhankintakeinojen avulla puututaan erityisesti yksityishenkilön yksityiselämän suojaan silloin, kun puuttuminen tapahtuisi kansallisen turvallisuuden suojaamiseksi ja olisi välttämätöntä demokraattisessa yhteiskunnassa[134]. Välttämättömyyden arviointikriteeriä on sittemmin täsmennetty muun muassa EIT:n ratkaisussa Szabó ja Vissy v. Unkari (12.1.2016), jossa tuomioistuin katsoi, että jäsenvaltioiden harkintamarginaalia puuttumisen välttämättömyydestä demokraattiselle yhteiskunnalle olisi tiukennettava siten, että puuttuminen mm. tietoliikenteeseen edellyttää ehdotonta välttämättömyyttä demokraattisten instituutioiden turvaamiseksi ja puuttuminen on ehdottoman välttämätöntä tärkeän tiedon hankkimiseksi yksittäisessä tapauksessa[135].

---

[132] HE 203/2017 vp, s. 275.
[133] HaVM 36/2018 vp, s. 95
[134] EIT tapaus Klass ja muut v. Saksa, 6.9.1978.
[135] EIT tapaus Szabó ja Vissy v. Unkari, 12.1.2016.

Edellä mainitun vuoksi tiedustelulakeihin tietoliikennetiedustelun käytön edellytyksiksi on säädetty yleisenä edellytyksenä tiedustelutoiminnan tuloksellisuus, joka on edellytyksenä kaikessa tietoliikennetiedustelun käytössä, mukaan lukien viestintäsalaisuuden piiriin kuulumattomaan valtiolliseen toimijaan tai siihen rinnastuvaan tahoon kohdistettavassa tietoliikennetiedustelussa[136]. Tuloksellisuuden lisäksi tiedustelun edellytyksenä on välttämättömyys tilanteissa, joissa tietoliikennetiedustelu kohdistuu henkilöön, joka nauttii luottamuksellisen viestin salaisuutta tai jos kohteena on sinänsä vieras valtio, mutta hakuehtojen käytön piiriin voi tulla muutakin tietoliikennettä[137]. Valtiollisiin toimijoihin tietoliikennetiedustelua kohdistettaessa riittää perusteeksi siis, että tietoliikennetiedustelun käytön tulee olla tarpeen tietojen hankkimiseksi vakavasti kansallisuutta turvallisuutta uhkaavasta toiminnasta (TtStL 4.2 § ja SotTiedL 68.1 §). Muihin kuin valtiollisiin toimijoihin tietoliikennetiedustelua kohdennettaessa tietoliikennetiedustelun tulee olla tarpeellisuuden lisäksi välttämätöntä eli että tietoja ei muilla tiedustelumenetelmillä saada hankittua (TtStL 4.1 § ja SotTiedL 70.1. §).

Tietoliikennetiedustelu kohdistuu Suomen alueella liikkuvaan, Suomen rajan viestintäverkossa ylittävään tietoliikenteeseen ja se eroaa ulkomaan tietojärjestelmätiedustelusta siten, että tiedustelu tapahtuu Suomen alueella[138]. Näin ollen tietoliikennetiedustelun kohteena voi olla esimerkiksi sellainen viestintä, joka tietoliikenteen reitittymisen vuoksi käy hetkellisesti Suomen rajojen sisäpuolella[139]. Ulkomaan tietojärjestelmätiedustelulla sen sijaan tarkoitetaan SotTiedL 62 §:ssä tietojen hankkimista teknisin menetelmin Suomen ulkopuolella olevista tietojärjestelmistä ja -verkoista Suomesta käsin. Tällöin viestintä ei reitity Suomen alueelle, vaan toiminta tapahtuu ulkomailla. Siviilitiedustelua koskevassa poliisilain 5 a luvussa ulkomaan tietojärjestelmätiedustelusta ei säädetä erikseen, sillä siviilitiedustelussa käytetään tältä osin lain 5 a luvun 11 § ja 14 §:ssä säädettyjä

[136] Sisäministeriö, 2018, s. 12.
[137] Sisäministeriö, 2018, s. 12–13.
[138] HE 203/2017 vp, s. 274.
[139] HE 203/2017 vp, s. 274.

teknisen kuuntelun ja laitetarkkailun menetelmiä[140]. Tietoliikennetiedustelun tekninen toteuttaminen on keskitetty Puolustusvoimien tehtäväksi ja SotTiedL 73 §:ssä ja TtStL 10 §:ssä säädetään Puolustusvoimien tiedustelulaitoksen tehtävästä toteuttaa tietoliikennetiedustelu teknisiltä osin suojelupoliisin puolesta.

Kun tietoliikenne- ja tietojärjestelmätiedustelu kohdistuu teknisin menetelmin välittyvästä tiedosta hankittavaan tietoon, henkilötiedustelu sen sijaan perustuu henkilökohtaiseen kanssakäymiseen taikka henkilön tai muun kohteen henkilökohtaiseen havainnointiin[141]. Tämä tarkoittaa tiedonhankintaa ihmisistä ja heidän hallussaan olevista asiakirjoista ja sähköisistä tallenteista muun muassa telekuuntelun, suunnitelmallisen tarkkailun, teknisen tarkkailun ja tietolähteen käyttämisen keinoin[142]. Henkilötiedustelun eri menetelmien käytön toimivaltuuksista säädetään siviilitiedustelussa poliisilain 5 a luvussa ja sotilastiedustelussa sotilastiedustelulain 4 luvussa. Sotilastiedustelussa hyödynnettävän henkilötiedustelun avulla on tarkoitus hankkia tietoa yksittäisen ihmisen, organisaation, tiedustelupalveluiden tai asevoimien toiminnasta ja intresseistä, jotka kohdistuvat Suomen maanpuolustukseen[143]. Siviilitiedustelussa henkilötiedustelulla pyritään selvittämään muun muassa henkilöiden ja organisaatioiden toimintaa, joka uhkaisi vakavasti Suomen kansallista turvallisuutta[144].

Nykymuotoisilla tiedustelumenetelmillä voidaan siis hankkia tietoa monenlaisista Suomen turvallisuusympäristöön ja maanpuolustukseen kohdistuvista kansallisista ja kansainvälisistäkin uhkista. Tällaisiksi uhkiksi voidaan lukea myös hybridiuhat, jotka koostuvat useista toisiaan täydentävistä vaikuttamiskeinoista. Kuten edellisessä 2.1.1 luvussa olen todennut, keinoja voivat olla esimerkiksi kyber- ja informaatiovaikuttaminen, vaalivaikuttaminen sekä poliittisiin päättäjiin ja heidän mielipiteisiinsä vaikuttaminen ja ylei-

[140] HE 203/2017 vp, s. 270; HE 202/2017 vp, s. 72.
[141] HE 202/2017 vp, s. 72; HE 203/2017 vp, s. 219.
[142] HE 203/2017 vp, s. 219; HE 202/2017 vp, s. 72.
[143] HE 203/2017 vp, s. 219.
[144] HE 202/2017 vp, s. 109.

sesti demokratian horjuttaminen kuin myös terrorismin ja aseellisen voimankäytön keinot. Nämä kaikki keinot voidaan nähdä uhkana kansalliselle turvallisuudelle tai sotilaalliselle maanpuolustukselle ja siten myös tiedustelutoimivaltuuksien käytön kohteina. Seuraavaksi tarkastelen, millä toimivaltuuksilla näihin hybridiuhkan osatekijöihin tiedustelutoiminnalla voidaan vastata.

2.2.3 Tiedustelutoimivaltuudet hybridiuhkien torjumiseksi

Siviilitiedustelun kohteista on säädetty samansisältöisin pykälin poliisilain 5 a luvun 3 §:ssä ja siviilitiedustelussa hyödynnettävän tietoliikennetiedustelun osalta TtStL 3 §:ssä, joten toimivaltuudet määräytyvät samoin perustein niin siviilitiedustelussa kuin siinä hyödynnettävässä tietoliikennetiedustelussa. Lisäksi sotilastiedustelun kohteista on säädetty SotTiedL 4 §:ssä. Tiedustelutoimintaa voidaan kohdistaa vain laissa tyhjentävästi säädettyihin kohteisiin eli uhkiin[145]. Tässä luvussa tiedustelutoimivaltuuksilla tarkoitetaan niitä tiedustelulakien toimivaltasäännöksiä, jotka mahdollistavat tiedonhankinnan jostain tietystä hybridivaikuttamisen tai -sodankäynnin keinosta eli uhasta. Sen vuoksi toimivaltuuksia lähdetään kuvaamaan tiedustelun kohteiden kautta.

Tässä kohtaa on tärkeää korostaa, että tiedustelutoiminnalla hankitaan tietoa tiedustelun kohteena olevista tahoista ja niiden toiminnasta, eivätkä tiedustelutoimivaltuudet itsessään anna tiedusteluviranomaisille toimivaltaa ryhtyä uhkien torjumiseen tai toiminnan estämiseen taikka muuten toimintaan vaikuttamiseen, vaan tiedustelutoiminnalla hankittujen tietojen pohjalta valtiojohto ja poliittiset päättäjät sekä toimivaltaiset viranomaiset voivat ryhtyä tarvittaviin toimenpiteisiin uhkien torjumiseksi ja estämiseksi. Esimerkiksi eduskunnan apulaisoikeusasiamies on 29.11.2013 ja 18.12.2003 antamissaan ratkaisuissa lähtenyt siitä, että laissa viranomaiselle määritelty tehtävä ei ole itsessään

[145] HaVM 35/2022 vp, s. 5.

toimivaltasäännös, vaan laissa tulee erikseen säätää viranomaisen toimivallasta toimintaan ryhtymiseksi[146]. Näin ollen esimerkiksi pelkkä PolHalL 10 §:ssä suojelupoliisille säädetty tehtävä hankkia tietoa kansallisen turvallisuuden suojaamiseksi ja muun muassa valtio- ja yhteiskuntajärjestystä tai sisäistä ja ulkoista turvallisuutta uhkaavien hankkeiden tai toimintojen havaitsemiseksi ei synnytä suojelupoliisille toimivaltuutta ryhtyä muihin toimiin uhkien torjumiseksi[147].

Sen sijaan tiedon hankkiminen käsittää myös tiedon tehokkaan hyödyntämisen ja toimittamisen ylimmälle valtiojohdolle tai toimivaltaiselle viranomaiselle toimiin ryhtymiseksi, jolloin esimerkiksi disinformaation levittämisen kohdalla voidaan ryhtyä vaikkapa ihmisten tilannetietoisuuden ja medialukutaidon parantamiseen ja heidän kouluttamiseensa, kun toiminnasta on saatu tiedustelumenetelmin ajankohtaista tietoa päätöksentekijöille[148]. Toki myös tiedusteluviranomainen voi olla uhkan estämiseen ryhtyvä toimivaltainen viranomainen, jos kyseisestä toimivaltuudesta on erikseen säädetty laissa.

Tiedustelun kohteita on syytä tarkastella lakien esitöiden kautta, koska niissä tiedustelun mahdollisten kohteiden toimintaa on kuvattu tarkemmin kuin lain säännöksissä. Keskityn tässä kohtaa vain hybridiuhkatematiikan kannalta keskeisiin tiedustelun kohteisiin tutkielman tavoitteiden mukaisesti, jotta voin vastata ensimmäiseen tutkimuskysymykseeni tiedusteluviranomaisten toimivaltuuksista liittyen hybridiuhkien torjumiseen. Sotilastiedustelua koskevan lain esitöissä on myös korostettu, että kaikkia tiedustelun kohteita ei voida eritellä pelkästään siviili- tai sotilastiedustelun alaisiksi, vaan voi olla tarpeellista, että tiedusteluviranomaiset hankkivat tietoa samasta kohteesta omalta osa-alueeltaan[149]. Tällaiset tilanteet ovat tyypillisiä hybridiuhkaan tähtäävän toiminnan yhteydessä, jolloin vaikutustoiminta pyritään salaamaan niin, että sitä ei pystytä yhdistämään toimin-

[146] EOAK 1870/2013, s. 11 ja EOAK 1634/4/01, s. 2.
[147] HE 202/2017 vp, s. 70.
[148] HE 203/2017 vp, s. 179.
[149] HE 203/2017 vp, s. 182.

nan taustalla olevaan tahoon. Lisäksi toiminta voidaan pyrkiä toteuttamaan hybridisodankäyntinä, joka ei täytä aseellisen konfliktin kynnystä tai esimerkiksi naamioimaan toiminta osittain terrorismilta vaikuttavaksi toiminnaksi.

Edellä kuvattuun piiloteltuun toimintaan voidaan sotilastiedustelun toimivaltuuksilla vastata, kun vieraan valtion asevoimat tai niihin rinnastuvat järjestäytyneet joukot ovat mukana toiminnassa tai niiden käyttöönottoa toimintaan liittyen suunnitellaan (SotTiedL 4.1 § 1 kohta). Tällöin toiminnan on oltava luonteeltaan sotilaallista, mutta sen ei täydy aiheuttaa välitöntä sotilaallista uhkaa Suomelle, vaan tietoa voidaan hankkia jo ennakolta[150]. Siviilitiedustelun toimivaltuudet sen sijaan mahdollistavat tiedonhankkimisen siltä osin, kun toiminta näyttäytyy terroristisena toimintana eikä sotilaallisena toimintana (PolL 5 a:3.1). Näin tiedustelutoimivaltuuksia yhdessä hyödyntämällä toiminnasta voidaan saada rakennettua parempi kokonaiskuva ja selvittää toiminnan todellinen luonne ja taho sen taustalla. Myös EIT on tapauksissa Klass ja muut v. Saksa (6.9.1978) sekä Weber ja Saravia v. Saksa (29.06.2006) katsonut, että niin sotilaallinen maanpuolustus, terrorismin torjunta kuin laittoman tiedustelutoiminnan ja vakoilun torjunta kuuluvat kansallisen turvallisuuden piiriin[151]. Näiden kansallista turvallisuutta uhkaavien toimien selvittämiseen tarvitaan niin sotilas- kuin siviilitiedustelun toimivaltuuksia.

On tärkeää huomata, että sotilastiedustelun kohteena oleva toiminta ei ole rikoksen valmisteluun liittyvää toimintaa eikä sitä ole säädetty rangaistavaksi, joten toiminta voi olla täysin laillista[152]. Myös siviilitiedustelussa tiedustelun kohteena olevan toiminnan tulee uhata kansallista turvallisuutta, mutta toiminta ei voi liittyä epäiltyyn tai oletettuun rikokseen, sillä rikoksiin liittyvään toimintaan ei voida siviilitiedustelun menetelmin ja toimivaltuuksin puuttua, vaan siltä osin kokonaisuuteen tulee soveltaa poliisilain 5 luvun salaisia tiedonhankintakeinoja[153]. Puolustusvoimien toimivaltuuksista rikosten ennalta

[150] HE 203/2017 vp, s. 183.
[151] EIT tapaus Klass ja muut v. Saksa, 6.9.1978, s. 18 ja EIT tapaus Weber ja Saravia v. Saksa, 29.06.2006, s. 7–8.
[152] HE 203/2017 vp, s. 181.
[153] HE 202/2017 vp, s. 172.

estämiseen, paljastamiseen ja selvittämiseen säädetään erikseen sotilaskurinpidosta ja rikostentorjunnasta puolustusvoimissa annetussa laissa. Tiedustelun kohteena oleva toiminta voi myös muuttua laittomaksi rikosperusteiseksi toiminnaksi, jolloin niin ikään tiedustelutoimivaltuudet eivät enää päde, vaan kyseeseen tulee rikosperusteinen sotilasvastatiedustelu tai siviilitiedustelun osalta rikosten selvittämiseen tai torjumiseen sovellettavat toimivaltuudet. Tiedustelun kohteena voi siis olla laajempikin kokonaisuus, johon tarvitaan niin rikosperusteisia tiedonhankintakeinoja kuin tiedustelumenetelmin toteutettavaa tiedonhankintaa.

Merkittävin hybridivaikuttamisen osa-alue tiedustelutoiminnan kannalta on kriittiseen infrastruktuuriin vaikuttamisen keinot, joihin tiedustelulakien esitöissä on viitattu muun muassa vieraiden valtioiden tiedustelun, yhteiskunnan elintärkeiden toimintojen lamauttamiseen tai keskeyttämiseen tähtäävän toiminnan ja tietoverkkoihin kohdistuvien kyberhyökkäyksien osalta. Elintärkeiden toimintoja ja huoltovarmuutta uhkaavaa toimintaa voi olla PolL 5a luvun 3.1 §:n 2 kohdassa mainittu vieraan valtion tiedustelu, jos tiedonhankinnan kohteena on vaikkapa Suomen energiapolitiikka, yhteiskunnan kriisinsietokyky, huoltovarmuus tai Suomen sotilaallinen valmius ja näistä saaduilla tiedoilla pyritään vaikuttamaan Suomen päätöksentekoon näistä kohteista[154].

Suomen sotilaalliseen valmiuteen ja muutoin Suomen maanpuolustukseen kohdistuvaan vieraan valtion tiedusteluun kohdistettavaan tiedonhankintaan sen sijaan annetaan toimivaltuudet SotTiedL 4.1 §:n 2 kohdassa. Elintärkeitä toimintoja ja huoltovarmuutta uhkaavaa toimintaa voidaan toteuttaa vieraan valtion tiedustelun lisäksi myös muilla keinoilla, joihin voidaan vastata siviilitiedustelussa PolL 5a luvun 3.1 §:n 6 kohdan toimivaltuuksilla ja sotilastiedustelussa SotTiedL 4.2 §:n toimivaltuuksilla. Näiden säännösten toimivaltuudet kattavat tiedustelun kybervaikuttamisesta sekä yhteiskunnan keskeisten toimintojen, kuten sähköntuotannon, tietoliikenteen tai rahoitus- ja maksujärjestelmien, lamauttamiseen tai tuhoamiseen tähtäävästä toiminnasta[155].

---

[154] HE 202/2017 vp, s. 173.
[155] HE 202/2017 vp, s. 175; HE 203/2017 vp, s. 191–192.

Kuten aiemmin on käynyt ilmi, hybridiuhissa voidaan hyödyntää myös informaatiovaikuttamista, jonka keinoja ovat esimerkiksi disinformaation levittäminen ja vaalivaikuttaminen. Siviilitiedustelussa PolL 5a:3.1 §:n 7 kohdassa annetaan toimivaltuus käyttää tiedustelumenetelmiä tiedonhankintaan vieraan valtion toiminnasta tai toiminnan valmistelusta, joka voi vahingoittaa Suomen taloudellisia tai muita tärkeitä etuja. Lain esitöissä tällaiseksi vahingoittavaksi toiminnaksi kuvataan muun muassa informaatiovaikuttaminen ja sen keinona disinformaatio-operaatiot, joilla pyritään vaikuttamaan kansalaismielipiteeseen niin Suomessa kuin muissakin maissa levittämällä väärää tietoa Suomen politiikasta[156]. Samoin SotTiedL 4.1 §:n 1 kohdan perusteluissa mainitaan informaatiovaikuttaminen ja disinformaatio, joista voitaisiin sotilastiedustelulla selvittää, onko toiminnan taustalla pyrkimyksiä ryhtyä sotilaalliseen voimankäyttöön joko tiedon levittäjän toimesta tai onko sen tavoitteena saada toinen ulkovalta ryhtymään sotilaallisiin toimiin Suomea kohtaan[157]. Vaalivaikuttaminen sen sijaan on tunnistettu PolL 5a:3.1 §:n 5 kohdan perusteluissa, joissa äänestämisen estäminen tai häiritseminen eduskuntavaaleissa tai presidentinvaalissa on esitetty kohdassa tarkoitettuna kansanvaltaista yhteiskuntajärjestystä uhkaavana toimintana[158].

Hybridivaikuttamisessa- ja sodankäynnissä voidaan pyrkiä vaikuttamaan valtiojohtoon ja päätöksentekijöihin esimerkiksi painostamalla, uhkaamalla tai korruptoimalla heitä. Siviilitiedustelussa toimivaltuudet tällaisen toiminnan suunnitteluun tai johtamiseen kohdistuvaan tiedonhankintaan on annettu niin ikään PolL 5a:3.1 §:n 5 kohdassa, jossa tarkoitettua kansanvaltaista yhteiskuntajärjestystä uhkaavaa toimintaa voi olla eduskunnan lainsäädäntövallan käyttämisen estäminen väkivaltaisesti tai hallitusvaltaa käyttävien

[156] HE 202/2017 vp, s. 175.
[157] HE 203/2017 vp, s. 185.
[158] HE 202/2017 vp, s. 174.

henkilöiden pakottaminen valtiollisten tehtävien tekemiseen tai tekemättä jättämiseen[159]. Samansuuntaisesta uhkaavasta toiminnasta tiedon hankkimiseen annetaan toimivaltuudet myös sotilastiedustelussa SotTiedL 4.1 §:n 1 kohdassa, jossa vieraan valtion tai siihen rinnastettavan toimijan toiminta kattaisi myös edellä kuvatut tilanteet[160].

Edellä mainittujen lisäksi tiedustelulait sisältävät monia tärkeitä toimivaltuuksia tiedon hankkimiseen esimerkiksi järjestäytyneen rikollisryhmän toiminnasta (PolL 5a:3.1,11) ja terrorismista sekä siihen liittyvästä väkivaltaisesta radikalisoitumisesta (PoL 5a:3.1,1). Samoin tietoa voidaan hankkia tunnuksettomien sotilaiden ja sotilasryhmittymien sekä vierastaistelijoiden toiminnasta ja toiminnan ohjaamisesta (PolL 5a:3.1,1) ja näiden lisäksi sotilastiedustelussa yleisesti valtiollisen tai ei-valtiollisen toimijan harjoittamasta sotilaallisesta toiminnasta (SotTiedL 4.1 § 1 kohta). Nämä toimet voivat olla osa hybridivaikuttamista tai -sodankäyntiä, joten on hyvä, että tiedustelun tarve myös tämänkaltaisesta toiminnasta on tiedostettu tiedustelulaeissa. Lisäksi kansainvälistä rauhaa ja turvallisuutta uhkaava toiminta voi tulla hybridiuhkan toteuttamisessa kysymykseen esimerkiksi autoritaaristen, puoliautoritaaristen tai hauraiden demokratioiden toimesta, jolloin ne pyrkivät rajoittamaan demokraattisten instituutioiden toimintaa ja perus- ja ihmisoikeuksien toteutumista[161]. Näin ollen näihinkin vastaaminen tiedustelutoimivaltuuksilla on tarpeellista ja ne on huomioitu PolL 5a luvun 3.1 §:n 8 kohdan sekä SotTiedL 4.1 §:n 5 kohdan perusteluissa.

Näin ollen voidaan todeta, että tiedustelulaeissa on omaksuttu hyvinkin kattavat toimivaltuudet tiedusteluviranomaisille tiedon hankintaan monenlaisista hybridiuhkan osatekijöistä. Olen tiivistänyt edellä kuvatut toimivaltuussäännökset vielä seuraavaan kuvioon 3, jossa niitä peilataan hybridiuhkan tekijöihin.

[159] HE 202/2017 vp, s. 174.
[160] Ks. HE 203/2017 vp, s. 184.
[161] HE 202/2017 vp, s. 175.

Informaatiovaikuttaminen	•SotTiedL 4.1 § 1 kohta •PolL 5a luvun 3.1 § 7 kohta
Kybervaikuttaminen	•SotTiedL 4.2 § •PolL 5 a luvun 3.1 § 6 kohta
Iskut yhteiskunnan kriittiseen infrastruktuuriin	•SotTiedL 4.2 § •PolL 5a luvun 3.1 § kohdat 1 ja 6
Vaalivaikuttaminen	•PolL 5a luvun 3.1 § 5 kohta
Valtiojohtoon ja päätöksentekijöihin vaikuttaminen	•SotTiedL 4.1 § kohdat 1 ja 2 •PolL 5a luvun 3.1 § kohdat 2 ja 5
Järjestäytynyt rikollisuus	•PolL 5a luvun 3.1 § 11 kohta
Terrorismi ja väkivaltainen radikalisaatio	•SotTiedL 4.2 § •PolL 5a luvun 3.1 § 1 kohta
Kansainvälistä rauhaa ja turvallisuutta uhkaava toiminta	•SotTiedL 4.1 § 5 kohta •PolL 5a luvun 3.1 § 8 kohta

Kuvio 3. Tiedusteluviranomaisten tiedonhankintatoimivaltuudet hybridiuhkan osatekijöistä.

Seuraavassa luvussa pohdin aluksi yleisesti viranomaisten oma-aloitteista tietojen antamista ja siihen liittyviä rajoituksia sekä sitä, mitkä säännökset säätävät tiedustelutoiminnalla saatujen tietojen antamisesta. Tavoitteenani on vastata toiseen tutkimuskysymykseeni ja selvittää miten tiedusteluviranomaiset voivat antaa oma-aloitteisesti tiedustelumenetelmin hankkimaansa tietoa toisille viranomaisille ja mitkä säännökset säätävät tiedusteluviranomaisten oma-aloitteisesta tietojen antamisesta. Pyrin tarkastelemaan nimenomaan edellä kuvattujen tiedustelutoimivaltuuksien nojalla saatujen, hybridiuhkaan viittaavien tietojen antamista oma-aloitteisesti ja selvittämään, miten oma-aloitteisen tietojen antamisen avulla voidaan torjua hybridiuhkia.

3 Oma-aloitteinen tietojen antaminen hybridiuhkien torjumiseksi

3.1 Viranomaisten oma-aloitteinen tietojen antaminen

Viranomaisen tietojen antamisesta puhuttaessa tarkoitetaan viranomaisen hallussa olevan tiedon luovuttamista toiselle viranomaiselle tämän niin pyytäessä ja toiminnasta käytetään yleisesti myös termiä tietojenvaihto. Toisinaan viranomainen voi kuitenkin antaa tietoja toiselle viranomaiselle myös oma-aloitteisesti ilman, että toinen viranomainen pyytää saada tiedot itselleen. Tavanomaisesti viranomaisten välinen tietojenvaihto tapahtuu asioiden käsittelyn yhteydessä ja on osa viranomaiselle säädettyä selvittämis- ja tutkintavelvollisuutta[162]. Tietojenvaihtoa voi tapahtua myös tilanteissa, joissa viranomainen tekee havainnon, joka liittyy toisen viranomaisen toimivaltaan tai tehtäviin kuuluvaan asiaan ja tällöin on kyse oma-aloitteisesta tietojen antamisesta tai laissa säädetystä tietojenantovelvollisuudesta[163].

Viranomaisten välisestä tietojenvaihdosta säädetään useissa erityislaeissa, mutta yleislakina tietojenvaihdossa tulee sovellettavaksi laki viranomaisen toiminnan julkisuudesta (621/1999) eli julkisuuslaki. Vaikka viranomaisten asiakirjojen julkisuutta pidetään oikeusvaltioissa pääasiallisena periaatteena, tulee tietojenvaihdossa kysymykseen julkisuutta rajoittavat, erityisesti henkilötietojen suojaa koskevat erityissääntelyt, joita ovat Euroopan unionin yleinen tietosuoja-asetus (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, myöhemmin tietosuoja-asetus)[164], tietosuojalaki (1050/2018), henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettu laki (1054/2018, rikosasioiden tietosuojalaki) sekä muut henkilötietojen käsittelyä koskevat erityissääntelyt. Näistä erityissääntelyistä keskeisimmät tämän tutkimuksen

[162] Kurvinen ja muut, 2023, s. 11. Esimerkiksi viranomaisen selvittämisvelvollisuudesta säädetään hallintolain 31 §:ssä ja esitutkinnan toimittamisesta säädetään esitutkintalain (805/2011) 3 luvun 3 §:ssä. Rajavartioviranomaisten ja tulliviranomaisten esitutkintatoimivallasta säädetään erikseen laeissa rikostorjunnasta Rajavartiolaitoksessa (108/2018) ja rikostorjunnasta Tullissa (623/2015).
[163] Kurvinen ja muut, 2023, s. 11.
[164] EUVL N:o L 119, 27.4.2016.

kannalta ovat laki henkilötietojen käsittelystä Puolustusvoimissa (332/2019) sekä laki henkilötietojen käsittelystä poliisitoimessa (616/2019). Lisäksi julkisuutta ja tiedonsaantioikeutta viranomaisen hallussa olevasta tiedosta voidaan rajoittaa salassapitovelvoitteilla, joita ovat esimerkiksi JulkL 23 §:ssä säädetty viranomaisen asiakirjasalaisuus sekä 24 §:ssä säädetyt vaitiolovelvollisuus sekä hyväksikäyttökielto[165]. Näiden yleisten salassapitovelvoitteiden avulla viranomaisen hallussa olevien tietojen yleistä julkisuutta voidaan rajoittaa yhteiskunnan tai yksityisen keskeisten intressien suojaamiseksi[166].

Lähtökohtaisesti viranomaisten tietojenvaihdossa noudatetaan siis julkisuusperiaatetta, jonka mukaan viranomaisten asiakirjat ovat julkisia ja jokaisella on oikeus saada tietoa viranomaisten toiminnasta ja julkisesta vallankäytöstä (JulkL 1§). Kuitenkin voimassa oleva salassapito- ja tietosuojasääntely voi muodostua esteeksi viranomaisten tietojenvaihdolle. Julkisuus on myös perustuslailla turvattu jokaiselle kuuluva perusoikeus, jonka mukaan viranomaisen hallussa olevat asiakirjat ja tallenteet ovat julkisia, jollei lailla ole erikseen säädetty välttämättömistä syistä julkisuuden rajoittamiseksi, ja jokaisella on oikeus saada tieto näistä asiakirjoista ja tallenteista (PL 12.2§). Julkisuus kohdistuu siis viranomaisen hallussa olevaan tallennettuun tietoon, sähköisiin tallenteisiin ja muihin viranomaisen asiakirjoihin, joista julkisuusperiaate velvoittaa viranomaisen antamaan tiedon yksityiselle[167]. Myös viranomaisen oikeus saada toisen viranomaisen hallussa olevia julkisia tietoa syntyy samoin perustein, kuin yksityisen oikeus näihin tietoihin[168]. Tästä asiakirjojen ja niiden sisältämien tietojen julkisuusolettamasta voidaan poiketa vain välttämättömistä syistä ja poikkeamisperusteista tulee säätää lailla[169].

Viranomaisten tietojenvaihtoon liittyvät termit eivät ole vakiintuneita eikä niitä käytetä johdonmukaisesti. Termillä tietojenvaihto viitataan viranomaiselta toiselle siirrettävään,

[165] Mäenpää, 2020a, s. 407.
[166] Mäenpää, 2017, s. 380.
[167] Mäenpää, 2017, s. 332.
[168] Huhtanen, 2010, s. 56.
[169] Mäenpää, 2017, s. 336–337.

luovutettavaan tai annettavaan tietoon, mutta tietojen luovuttaminen ja antaminen ilmenevät voimassa olevassa lainsäädännössä ja lakien esitöissä jokseenkin samoissa asiayhteyksissä eikä käsitteiden käytölle tehdä lainsäädännössä eroa[170]. Tietojen siirtämisen käsitettä käytetään taas erityisesti EU-lainsäädännössä ja sen toimeenpanemiseksi annetussa kansallisessa lainsäädännössä henkilötietojen siirron osalta[171]. Kurvinen ja muut ovat tulkinneet julkisuuslain 16 §:n perusteella, että tietojen antaminen on tietojen luovuttamista laajempi käsite, koska tietoja voidaan antaa myös muilla tavoin, kuin kopiona, tulosteena tai sähköisessä muodossa, kuten esimerkiksi suullisesti JulkL 16 §:n 1 momentin mukaisesti. Voisi ajatella, että tietojen luovuttaminen koskisi pyynnöstä tehtävää tietojen antamista, kun taas tietojen antaminen käsittäisi tilanteet, joissa viranomainen on velvoitettu antamaan tietoja toiselle viranomaiselle lain nojalla tai viranomainen antaisi tietoja oma-aloitteisesti[172]. Kuitenkin käsitteitä käytetään eri tavoin eri yhteyksissä ja tilanteissa ja niillä tarkoitetaan usein myös samaa asiaa, mikä tekee käsitteiden johdonmukaisesta käytöstä haastavaa.

Tietojenvaihto käsittää siis tietojen antamisen, jota käytän tässä tutkielmassa kaikkea tietojen antamista, luovuttamista ja siirtämistä koskevana käsitteenä. Tietojenvaihto tarkoittaa yleisesti viranomaisen velvollisuutta antaa toiselle viranomaiselle tämän pyytämä julkinen tieto, mutta se käsittää myös muutoin salassa pidettäväksi säädetyn tiedon antamisen toiselle viranomaiselle tietyissä tilanteissa, joissa tietojen antaminen katsotaan tarpeelliseksi tai jopa viranomaisen velvollisuudeksi[173]. Esimerkiksi lastensuojelulain (417/2007) 25.1 §:ssä luetelluilla viranomaisilla on velvollisuus salassapitosäännösten estämättä ilmoittaa poliisille, kun heillä on syytä epäillä, että lapseen on kohdistettu

[170] Kurvinen ja muut, 2023, s. 12.
[171] Hallituksen esityksessä rikosasioiden tietosuojalaiksi tietojen siirtämiseksi katsottaisiin henkilötietojen saattaminen kansainväliselle tai kolmannessa maassa sijaitsevalle taholle. Siirtäminen tapahtuisi sähköisen palvelun välityksellä, kuten sähköpostitse tai avaamalla katseluoikeus sähköiseen palveluun tallennettuihin tietoihin. Tietojen luovuttaminen taas tarkoittaisi rekisterinpitäjän toimesta tietojen luovuttamista toiselle rekisterinpitäjälle, joka voi käsitellä tietoja omiin käyttötarkoituksiinsa, mikä osaltaan olisi myös henkilötietojen siirtämistä. HE 31/2018 vp, s. 59.
[172] Kurvinen ja muut, 2023, s. 12.
[173] Määttä & Hirvonen, 2018, s. 8.

säännöksessä tarkoitettu rikos (25.3 §). Tällaisissa tilanteissa viranomainen antaa poliisille salassa pidettäväksi säädettyjä henkilötietoja tiedonantovelvollisuuden nojalla. Perustuslakivaliokunta on lausuntokäytännössään useasti korostanut, että salassa pidettävän tiedon antaminen edellyttää kuitenkin vain välttämättömien tietojen luovuttamista tai tietojen saamisen tarpeellisuutta johonkin tarkoitukseen, ja nämä edellytykset tulee olla kirjattuna lakiin. Lisäksi jonkin tarkoituksen vuoksi tarpeellisten tietojen sisältö tulee olla täsmällisesti rajattu laissa.[174]

Viranomaisten välisellä tietojenvaihdolla voidaan edistää hallintolain 10 §:ssä säädettävän viranomaisten välisen yhteistyön toteutumista, sillä pykälän mukaan viranomaisen on toimivaltansa rajoissa ja asiaan kuuluvassa laajuudessa avustettava pyynnöstä toista viranomaista hallintoasian hoitamisessa ja edistettävä muutoinkin viranomaisten keskinäistä yhteistyötä[175]. Kuitenkaan tämä yhteistyövelvoite ei oikeuta viranomaista yleiseen tietojen antamiseen, vaan yhteistyössä on noudatettava muun muassa julkisuuslain säännöksiä, jotka koskevat tietojen luovuttamista toiselle viranomaiselle sekä henkilötietojen suojaa koskevaa sääntelyä[176]. Erityisesti salassa pidettävää tietoa voidaan antaa toiselle viranomaiselle vain, kun se on julkisuuslain 29 §:ssä säädetyissä tilanteissa tai muiden lakien säännöksissä sallittu[177]. Esimerkiksi henkilötietojen käsittelystä Rikosseuraamuslaitoksessa annetun lain (1301/2021) 5 luvussa on säädetty tietyistä tilanteista, joissa Rikosseuraamuslaitos saa salassapitosäännösten estämättä luovuttaa henkilötietoja toisille viranomaisille, kuten suojelupoliisille ja Puolustusvoimille, joko pyynnöstä tai oma-aloitteisesti.

Tietojen antaminen on siis osa viranomaisten välistä yhteistyötä, vaikka HL 10 § ei annakaan rajoituksetonta tietojenvaihto-oikeutta viranomaisten välille. Määtän ja Hirvosen mukaan passiivinen viranomaisten välinen yhteistyö sisältää tietojen antamisen toiselle

---

[174] Ks. esim. PeVL 1/2015 vp, s. 2 ja PeVL 21/2020 vp, s. 5.
[175] Viranomaisyhteistyöstä säädetään myös erityislaeissa, esimerkiksi poliisin, Tullin ja Rajavartiolaitoksen yhteistyöstä annetussa laissa (687/2019, PTR-laki).
[176] Mäenpää, 2020a, s. 260.
[177] Heuru, 2003, s. 310.

viranomaiselle joko tämän pyynnöstä tai oma-aloitteisesti. Aktiivinen viranomaisyhteistyö sen sijaan käsittää viranomaisten yhteisen tilannekuvan ylläpitämisen ja muunlaiset yhteiset toimet ja operaatiot, jollaista esimerkiksi poliisin, Tullin ja Rajavartiolaitoksen yhteistyö rikosten ehkäisemiseksi ja torjumiseksi PTR-toiminnassa on[178]. Kokonaisturvallisuuden sanastossa tilannekuva määritellään kootuksi kuvaukseksi vallitsevista olosuhteista, tapahtumista ja tekijöistä tietyssä tilanteessa. Tilannekuva koostuu vallitsevan tilanteen kuvauksen lisäksi tilanteeseen johtaneiden taustatietojen ja tilanteen kehittymisen selvittämisestä ja arvioinnista ja siihen pyritään kokoamaan eri toimijoiden toimintavalmiudet nykyisessä tilanteessa sekä tilanteen mahdollisissa kehitysvaiheissa.[179] Tilannekuvan tarkoituksena on siis pysyä tietoisena yhteiskuntamme toimijoiden toimintavalmiuksista ja niihin vaikuttavista tekijöistä kussakin tilanteessa. Tilannekuva voi olla koottu kaikkien yhteiskunnan toimijoiden toimintavalmiuksista tai se voi keskittyä tiettyyn toimialaan ja toimintaympäristöön, kuten kyberturvallisuuteen.

Viranomainen voi siis tietyissä tilanteissa antaa tietoa oma-aloitteisesti ja joissain tilanteissa viranomainen on myös velvollinen antamaan tietoa toiselle viranomaiselle. Jotta voin vastata toiseen tutkimuskysymykseeni tiedusteluviranomaisten oma-aloitteisen tietojen antamisen toimivaltuuksista, tulee ensin selvittää yleisesti viranomaisten tietojen antamista koskevat säännökset ja milloin tietojenantovelvollisuudesta tai -oikeudesta säädetään erityislailla.

3.1.1 Yleinen tietojen antaminen

Yleislakina viranomaisten tietojen antamisessa toimii siis julkisuuslaki ja sen säännökset viranomaisten asiakirjojen ja tietojen julkisuudesta sekä salassapidosta. Jokainen voi

[178] Määttä & Hirvonen, 2018, s. 8. PTR-toiminnassa poliisin, Tullin ja Rajavartiolaitoksen virkamiehet voivat suorittaa tietyissä tilanteissa toisen viranomaisen toimivaltaan kuuluvia tehtäviä, käyttää yhteisiä rekistereitä ja suorittaa yhteistä tiedustelu- ja analyysitoimintaa. Ks. laki poliisin, Tullin ja Rajavartiolaitoksen toiminnasta (687/2009).
[179] Kokonaisturvallisuuden sanasto, 2017, s. 64.

saada tietoa julkisesta asiakirjasta julkisuusperiaatteen mukaisesti eikä tiedon käyttötavalla ole merkitystä tiedon saamisoikeuden kannalta, ellei muussa lainsäädännössä säädetä toisin[180]. Lisäksi viranomaisilla on velvollisuus yleisesti edistää tiedonsaantioikeuden toteutumista[181]. Koska julkisuus on lähtökohta viranomaisen toiminnassa ja sen asiakirjoissa, voidaan julkisuusolettamasta poiketa vain välttämättömistä syistä laintasoisen säännöksen perusteella ja yleiset julkisuudesta poikkeavat salassapitovelvoitteet on kirjattu julkisuuslain 24.1 §:ään. Näin ollen viranomaiset eivät voi oman harkintansa puitteissa päättää asiakirjan ja sen tietojen julkisuudesta tai julkisuuden rajoittamisesta[182]. Myöskään julkisuuden rajoittaminen ei määräydy viranomaiselle toimitetun asiakirjan laatijan tai lähettäjän vaatimuksen pohjalta, vaan viranomainen arvioi sen julkisuuden tai salassa pidettävyyden objektiivisesti julkisuuslain perusteella[183]. Korkein hallinto-oikeus on tapauksissa 2017:82 ja 2019:83 katsonut, että pyydettyjen asiakirjojen julkisuutta ja salassa pidettävyyttä tulee arvioida riippumattomasti julkisuuslain pohjalta, eikä niitä voida pitää salassa ainoastaan yrityksen tahtotilaan tai esittämään selvitykseen liikesalaisuudesta vedoten[184]. Julkisuutta voidaan kuitenkin rajoittaa julkisuuslakiin ja erityislainsäädäntöön kuuluvilla salassapitosäännöksillä. Sen lisäksi tiedonsaantioikeutta voidaan rajoittaa tiedon luovuttamista rajoittavilla säännöksillä[185].

Yleinen tiedonantovelvollisuus kohdistuu lähtökohtaisesti viranomaisen julkisiin asiakirjoihin, sillä lähtökohtaisesti julkisuuslain 22 §:ssä säädetään kiellosta antaa tietoa salassa pidettävistä asiakirjoista sivullisille. Myös toiset viranomaiset katsotaan sivullisiksi, jolloin viranomaisella ei ole yleistä oikeutta saada salassa pidettäväksi määrättyä tietoa toiselta viranomaiselta, vaan julkisuuslain salassapitoperusteet rajoittavat myös viranomaisten välistä tietojen luovuttamista[186]. Asiakirja voidaan määrätä salassa pidettäväksi

[180] Neuvonen, 2014, s. 165.
[181] Kulla, 2012, s. 339.
[182] Mäenpää, 2002, s. 134.
[183] Mäenpää, 2023, s. 682.
[184] KHO 2017:82 ja KHO 2019:83.
[185] Voutilainen, 2021, s. 677.
[186] Mäenpää, 2020a, s. 248–249.

julkisuuslain säännösten tai erityislakien säännösten perusteella, joita tarkastelen tarkemmin myöhemmin. Perustuslakivaliokunta on useaan otteeseen painottanut, että viranomaisten tietojen salassapitoa koskevat säännökset tulisi sisällyttää yleislakiin ja niiden viemistä erityislainsäädäntöön tulisi välttää, kuten eduskunta on nykyistä julkisuuslakia uudistettaessa vuonna 1998 edellyttänyt[187]. Kuitenkin salassapidosta ja siitä poikkeamisesta tietyissä tilanteissa säädetään useissa erityislaeissa, mutta erityislakien säännökset tukevat julkisuuslain 7 luvun vaatimuksia säätää lailla nimenomaisesti tiedonsaamisoikeudesta ja tiedonantovelvollisuudesta. Lähtökohtaisesti kaikki julkisuuslain 24.1 §:ssä säädetyt viranomaisen asiakirjat ovat siis salassa pidettäviä, jollei erityislaissa säädetä tilanteista, joissa salassapidosta voidaan poiketa.

Viranomaisen yleinen tiedonsaantioikeus toisen viranomaisen julkisiin asiakirjoihin perustuu julkisuuslain 9 §:ään, jonka mukaan jokaisella on tiedonsaantioikeus viranomaisen julkisesta asiakirjasta. Tiedon saamiseksi tulee kuitenkin tehdä viranomaiselle julkisuuslain 13 §:n tarkoittama tietopyyntö viranomaisen asiakirjasta tai asiakirjassa olevasta tiedosta[188]. Julkisuuslain 16 §:ssä säädetään yleisistä viranomaisen asiakirjan antamistavoista, joita ovat tiedon antaminen asiakirjasta suullisesti, asiakirjan antaminen viranomaisen luona nähtäväksi ja jäljennettäväksi tai kuunneltavaksi tai antamalla asiakirjasta kopio tai tuloste. Tieto viranomaisen julkisesta asiakirjasta on annettava tietopyynnössä pyydetyllä tavalla, ellei se aiheuta kohtuutonta haittaa virkatoiminnalle (JulkL 16.1§). Julkisesta asiakirjasta tehtyyn tietopyyntöön tulee vastata mahdollisimman pian, tai viimeistään kahden viikon aikana tietopyynnön saannista ja jos pyydettyjä asiakirjoja on paljon tai niihin sisältyy esimerkiksi salassa pidettävää tietoa, tulee pyyntöön vastata viimeistään kuukauden kuluessa (JulkL 14.4§). Eduskunnan oikeusasiamies on myös 29.1.2020 antamassaan ratkaisussa huomauttanut, että laissa säädetyistä määräajoista

[187] PeVL 62/2018 vp, s. 9; PeVL 2/2008 vp, s. 2. Ks. myös julkisuuslain valmisteluasiakirjat EV 303/1998 vp, s. 1 ja HaVM 31/1998 vp, s. 7.

[188] Neuvonen, 2017, s. 101. Julkisuuslain tarkoittamaksi asiakirjaksi katsotaan paperille tallennetut kirjallisen asiakirjat, jotka voivat sisältää myös kuvallisia esityksiä sekä sähköiset tallenteet, kuten digitaaliset asiakirjat ja audiovisuaaliset tallenteet, joiden sisältö saadaan selville erilaisin apuvälinein, kuten esimerkiksi äänen- tai kuvantoistolaitteiden avulla. Viranomaisen asiakirja on jotakin käyttötarkoitusta varten laadittu kokonaisuus. (Mäenpää, 2023, s. 649; Neuvonen, 2017, s. 67).

ei voi poiketa esittämällä viivästymiselle perusteita, kuten valmistelijoiden loman sijoittumisen tietopyyntöön vastaamisen määräajalle[189].

Julkisuuslaissa säädetään siis yleisistä viranomaisen asiakirjan salassapitoperusteista sekä viranomaisten julkisista asiakirjoista, joihin pätee yleinen tiedonsaamisoikeus sekä viranomaisen velvollisuus antaa tieto julkisesta asiakirjasta pyynnöstä ja myös tiedottaa esimerkiksi keskeneräisten asiakirjojen sisällöstä ja toiminnastaan avoimuuden lisäämiseksi (JulkL 19–20§). Viranomaisella on kuitenkin velvollisuus antaa tieto myös asiakirjasta, joka sisältää julkisen tiedon lisäksi lailla salassa pidettäväksi säädettyä tietoa, jos tiedon antaminen on mahdollista niin, ettei salassa pidettävä osuus tule tietoon (JulkL 10 §). Tätä kutsutaan osajulkisuudeksi, mikä tarkoittaa, että salassapitovelvoite kohdistuu vain osaan tai osiin asiakirjasta ja muuten asiakirja on julkinen[190].

Korkein hallinto-oikeus on ottanut kantaa sellaisten asiakirjojen antamiseen, jotka sisältävät sekä julkista että salassa pidettävää tietoa tapauksissa KHO 2007:39 ja KHO 2015:163. KHO on tapauksessa 2007:39 katsonut, että ylioppilastutkintolautakunnan oli toimitettava siltä pyydetyt tiedot ylioppilastutkinnon tulosluettelosta siltä osin, kun henkilötiedot ja muut salassa pidettävät tiedot oli mahdollista teknisesti poistaa ilman uuden viranomaisen asiakirjan laatimiseen rinnastettavia toimenpiteitä[191]. Tapauksessa 2015:163 KHO oli sen sijaan katsonut julkisuuslain 10 §:n nojalla, että Pääesikunnalla ei ollut velvollisuutta antaa pyydettyjä asiakirjoja, jotka sisälsivät sekä julkisuuslain 24.1 §:n 10 kohdan perusteella salassa pidettäviä maanpuolustusta koskevia tietoja sekä julkisia tietoja, koska asiakirjojen sisältö ei olisi salassa pidettävien tietojen peittämisen jälkeen enää ollut asianmukaisesti ymmärrettävissä[192]. Jälkimmäinen päätös tukee julkisuuslain valmistelussa korostettua ymmärrettävyysvaatimusta, jonka mukaan viranomainen ei voi toteuttaa osajulkisuutta, jos julkisten tietojen pohjalta asiakirjasta saa harhaanjohta-

[189] EOAK/811/2019, s. 3.
[190] Mäenpää, 2020a, s. 157.
[191] KHO 2007:39.
[192] KHO 2015:163.

van tai asiallisesti virheellisen käsityksen eikä sen sisältö siten ole ymmärrettävissä oikein[193]. Kun viranomainen antaa asiakirjapyynnön pohjalta tiedon vain asiakirjojen julkisista osista, tulee viranomaisen kertoa tiedonpyytäjälle, miksi se on kieltäytynyt antamasta osan pyydetyistä tiedoista sekä noudattaa muita julkisuuslain 14.3 §:ssä säädettyjä menettelyllisiä toimenpiteitä. Apulaisoikeuskansleri on 20.9.2013 antamassaan ratkaisussa katsonut, että viranomainen oli toiminut julkisuuslain 14.3 §:n velvoitteiden vastaisesti, kun viranomainen ei ollut kertonut asiakirjan pyytäjälle peittäneensä tietoja toimittamistaan asiakirjoista eikä perustetta tietojen peittämiselle[194].

Näin ollen lähtökohtaisesti julkisesta viranomaisen asiakirjasta voidaan antaa tieto niin yksityiselle kuin toiselle viranomaisellekin ja salassa pidettävää tietoa sisältävästä asiakirjasta ei pääsääntöisesti voida antaa tietoa. Julkisuuslain 26 § kuitenkin säätää yleisistä perusteista salassapitovelvoitteesta poikkeamiseen ja niiden lisäksi salassapidosta poikkeamisesta säädetään lukuisissa erityislaeissa. Seuraavaksi käsittelen erityistä tietojen antamista, joka pääasiassa tarkoittaa salassapidosta poikkeamista ja salassa pidettävän tiedon antamista joko julkisuuslakiin kirjattujen erityisten perusteiden nojalla tai erityislakien säännösten nojalla.

3.1.2 Erityinen tietojen antaminen

Tietojen antamisesta säädetään julkisuuslain lisäksi myös monissa erityislaeissa, joiden säännökset velvoittavat viranomaisia. Laissa on voitu esimerkiksi säätää siten, että viranomaiset eivät voi antaa salassa pidettävää tietoa erityisesti silloin, kun viranomaisen tiedot kuuluvat perustuslailla turvatun yksityiselämän suojan piiriin (PL 10§). Kuitenkin myös viranomaisten asiakirjojen salassapitoon liittyy rajoituksia ja salassapidosta poikkeamisen yleisistä perusteista on säädetty julkisuuslain 26 §:ssä. Näiden salassa pidettävien tietojen antamisesta toiselle viranomaiselle taas on säädetty julkisuuslain 29 §:ssä.

---

[193] Mäenpää, 2023, s. 698. Ks. myös HE 30/1998 vp, s. 65.
[194] OKV/322/1/2012, s. 3.

Erityislaeissa sen sijaan säädetään erityisistä tilanteista, joissa viranomaisella on oikeus saada tai velvollisuus antaa salassa pidettävää tietoa, jolloin säännöksillä poiketaan kyseisten asiakirjojen pääsääntöisestä salassa pidettävyydestä.

Pääosin viranomaisen oikeus saada salassa pidettävää tietoa määräytyy useissa erityislaeissa säädetyn pohjalta, jolloin laissa tulee nimenomaisesti säätää viranomaisen oikeudesta saada salassa pidettävä tieto tai viranomaisen oikeudesta tai velvollisuudesta antaa salassa pidettävä tieto[195]. Näin ollen salassapidosta poikkeamisesta tulee säätää laintasoisella säädöksellä, eikä siten esimerkiksi säädetyllä asetuksella voida poiketa salassapidosta. Erityislain säännöksestä tulee käydä ilmi, että tietoa voidaan luovuttaa salassapitosäännöksistä riippumatta sekä ne salassapitoperusteet, jotka säännös syrjäyttää[196]. Nämä laintasoiset erityissäännökset syrjäyttävät julkisuuslain säännökset, mutta useimmiten erityislainsäädännössä säädetään poikkeuksia vain joihinkin julkisuuden lohkoihin, joita erityislain salassapito koskee tai tilanteisiin, joissa yleisestä julkisuuslain säätämästä salassapidosta poiketaan ja muilta osin julkisuuslaki täydentää sääntelyä[197]. Näin ollen julkisuuslakia voidaan soveltaa täydentävästi aina, kun erityislakiin ei ole sisällytetty yleislaista poikkeavaa säännöstä[198].

Julkisuuslain säännökset ohjaavat yleistä poikkeamista asiakirjojen salassapidosta ja lain 26 §:ssä onkin säädetty yleisistä perusteista, joiden pohjalta viranomainen voi antaa tiedon salassa pidettävästäkin asiakirjasta. Lain 26.1 §:n mukaan viranomainen voi antaa tiedon salassa pidettävästä asiakirjasta, jos tiedon antamisesta tai tiedonsaamisoikeudesta on nimenomaisesti säädetty laissa tai jos asiakirjan salassapidolla suojattu taho antaa siihen suostumuksensa. Lisäksi viranomainen voi antaa tiedon lain 26.2 §:ssä mainituista seikoista, kuten sosiaalihuollon asiakkuudesta, jos tieto on tarpeen laissa säädetyn yksityisen tai viranomaisen tiedonantovelvollisuuden toteuttamiseksi tai tiedot antavan viranomaisen toimivaltaan kuuluvan korvauksen tai vaatimuksen toteuttamiseksi.

---

[195] Krakau & Haapalehto, 2020, s. 131.
[196] Krakau & Haapalehto, 2020, s. 132.
[197] Kulla, 2012, s. 343.
[198] HE 30/1998 vp, s. 47.

Julkisuuslain 26.3 §:n mukaan viranomainen voi antaa tiedon suorittaakseen antamansa virka-aputehtävän tai muun lukuunsa suoritettavan toimeksiannon tai tehtävän, jos se on välttämätöntä tehtävän suorittamiseksi. Tietoja voidaan luovuttaa näitä tehtäviä varten myös silloin, kun salassa pidettävien tietojen poistaminen ei ole tarkoituksenmukaista esimerkiksi tietojen suuren määrän vuoksi ja kun tietoja antava viranomainen on varmistunut tietojen asianmukaisesta salassapidosta ja suojaamisesta myös tietoja saavassa viranomaisessa (JulkL 26.3 §).

Julkisuuslain 27–30 §:t sisältävät myös erityisiä perusteita, joilla voidaan antaa salassa pidettävää tietoa. Nämä erityiset perusteet liittyvät arkistoidun salassa pidettävän asiakirjan luovuttamiseen tutkimuskäyttöön (27 §), yksittäistapauksessa viranomaisen myöntämään lupaan antaa asiakirjan tietoja tieteellisen tutkimuksen, tilastoinnin tai viranomaisen suunnittelu- tai selvitystyötä varten (28 §), toisen viranomaisen lakiin kirjattuun tiedonsaantioikeuteen (29 §) sekä kansainvälisen yhteistyön toteuttamiseen (30 §). Näistä erityisistä perusteista tämän tutkimuksen kannalta merkittävimmät ovat 29 §:ssä säädetyt perusteet antaa tietoa toiselle viranomaiselle, ja ne ovat osittain hyvin samansuuntaiset 26 §:n yleisten poikkeamisperusteiden kanssa. Julkisuuslain 29.1 §:n mukaan viranomainen voi antaa tiedon salassa pidettävästä asiakirjasta toiselle viranomaiselle, jos tiedonantovelvollisuudesta tai tiedonsaamisoikeudesta on erikseen säädetty lailla, tai jos asianosainen antaa tiedon luovuttamiseen suostumuksensa, asiakirja on tarpeen oikeusturvamenettelyssä tai se on tarpeen viranomaiseen kohdistuvan valvonta- tai tarkastustehtävän suorittamiseksi. Lisäksi viranomainen voi antaa tiedon toiselle viranomaiselle JulkL 24.1 §:n 31 kohdassa salassa pidettäväksi säädetyistä osoite- tai muista yhteystiedoista (JulkL 29.2 §).

Kuten aiemmin on käynyt ilmi, viranomaisten väliseen tietojen antamiseen pätee samat perusteet kuin viranomaisen ja yksityisenkin välillä, mutta viranomaisten tiedonsaanti on joustavampaa oikeusturvan toteutumisen ja viranomaisiin kohdistuvan valvonnan tehokkuuden, kuten virkavastuun toteutumisen, osalta[199]. Kuitenkaan salassapidosta ei voi

[199] Mäenpää, 2020a, s. 250.

poiketa vain siksi, että tieto olisi yleisesti tarpeellinen tai hyödyllinen toisen viranomaisen tehtävän hoitamiseksi[200]. Eduskunnan oikeusasiamies on ratkaisussaan 23.11.2018 korostanut, että salassa pidettävien tietojen antamiseen toiselle viranomaiselle on aina oltava laissa säädetty peruste eikä yhteiskunnallisesti hyväksyttävä peruste, tässä tapauksessa järjestäytyneen rikollisuuden estäminen, mahdollista sääntelystä poikkeamista[201]. Lisäksi viranomaisen on julkisuuslain 13.2 §:n mukaan perusteltava pyyntönsä saada tietoa salassa pidettävästä asiakirjasta ja ilmoitettava tiedon käyttötarkoitus ja peruste tiedon saamiseksi. Viranomainen, jonka hallussa salassa pidettävää tietoa sisältävä asiakirja on, päättää tiedon antamisesta toiselle viranomaiselle, eikä viranomaisella näin ollen ole ehdotonta oikeutta saada tietoa, vaikka salassapidosta poikkeamiselle on olemassa edellytykset[202].

Erityislaeissa tietojen antamista koskevat säännökset on muotoiltu osin tietojenantovelvollisuutta koskeviksi, jolloin ne asettavat viranomaisille velvollisuuden antaa toiselle viranomaiselle tämän pyytämiä tietoja, kun taas osa erityislakien säännöksistä on muotoiltu viranomaisen tiedonsaantioikeutta koskeviksi, jolloin viranomaisella on oikeus saada pyytämänsä tiedot toiselta viranomaiselta[203]. Lisäksi erityislaissa on voitu säätää viranomaisen oikeudesta antaa tietoa toiselle viranomaiselle, jolloin salassa pidettävän tiedon antaminen perustuu tietoja antavan viranomaisen harkintaan[204]. Esimerkiksi sosiaali- ja terveydenhuollon valvonnasta annetun lain (741/2023) 46.2 §:ssä säädetään muun muassa viranomaisen oikeudesta ilmoittaa poliisille salassapitosäännösten estämättä välttämättömät tiedot henkeen tai terveyteen kohdistuvan uhkan arvioimiseksi ja uhkaavan teon estämiseksi. Ilmoitusoikeudessa on kyse oma-aloitteisesta tietojen anta-

[200] Mäenpää, 2020a, s. 251.
[201] EOAK/4963/2017, s. 4 ja 11.
[202] Mäenpää, 2020a, s. 252.
[203] Voutilainen, 2021, s. 679. Lisäksi Voutilainen on maininnut tietojen luovutusoikeuden, joka edellyttää viranomaisen tekemää pyyntöä tietojen saamiseksi, sekä suostumuksen perusteella tapahtuvan tietojen antamisen, jolla viitataan esimerkiksi asianomaisen suostumukseen antaa häntä koskevia salassa pidettäviä tietoja. Ks. myös julkisuuslain valmisteluasiakirjoista, HE 30/1998 vp, s. 15.
[204] Voutilainen, 2021, s. 679.

misesta, jolloin tietojen antaminen perustuu viranomaisen tekemään havaintoon tai saamaan tietoon, joka liittyy toisen viranomaisen tehtäväkenttään[205]. Tällöin viranomainen voi harkintavaltansa puitteissa antaa tietoa oma-aloitteisesti toiselle viranomaiselle ilman, että viranomainen on pyytänyt näitä tietoja[206]. Tällaiset harkinnanvaraisesta ilmoitusoikeudesta säätävät säännökset poikkeavat julkisuuslain 13 §:n edellytyksestä pyytää tieto viranomaisen asiakirjasta.

Viranomaisen tiedonantovelvollisuutta koskeva ilmoitusvelvollisuus on kirjattu esimerkiksi lastensuojelulakiin (417/2007), jonka 25.3 §:n mukaan lain 25.1 §:ssä mainituilla tahoilla ja viranomaisilla on velvollisuus ilmoittaa poliisille salassapitosäännösten estämättä, mikäli on syytä epäillä, että lapseen on kohdistettu esimerkiksi seksuaalirikoksena rangaistavaksi säädetty teko. Tällainen ilmoitusvelvollisuus perustuu laissa säädettyjen edellytysten täyttymiseen, eikä viranomaiselle tai muulle ilmoitusvelvolliselle taholle jää kovinkaan suurta harkintavaltaa tietojen antamiseen[207]. Tiedonsaantioikeudesta taas on säädetty esimerkiksi poliisilain 4 luvun 2 §:ssä, jonka mukaan poliisilla on oikeus saada viranomaiselta tehtäviensä suorittamiseksi tarpeelliset tiedot ja asiakirjat salassapitosäännösten estämättä.

Joissain erityissäännöksissä tietojen antaminen on rinnastettu myös virka-apuun tai viranomaisten välisen yhteistyön toteuttamiseen. Näin on esimerkiksi työtuomioistuimesta annetun lain (646/1974[208]) 46 §:ssä, jonka mukaan valtion, kunnan, hyvinvointialueen ja muun julkisoikeudellisen yhteisön viranomaiset ovat pyynnöstä velvoitettuja antamaan tietoja ja muuta virka-apua työtuomioistuimelle. Virka-aputehtävän suorittamiseen on viitattu myös aiemmin käsitellyssä julkisuuslain 26.3 §:ssä, jonka mukaan viranomainen voi antaa salassa pidettävää tietoa muun muassa silloin, jos se on välttämä-

[205] Kurvinen ja muut, 2023, s. 41.
[206] Mäenpää, 2023, s. 730.
[207] Kurvinen ja muut, 2023, s. 192.
[208] Lakia muutettu teknisin osin hyvinvointialueiden osalta lailla oikeudenkäynnistä työtuomioistuimessa annetun lain muuttamisesta 242/2023.

töntä viranomaisen antaman virka-aputehtävän suorittamiseksi. Erityissäännökset säätelevät nimenomaan tilanteita, joissa viranomaisella on joko velvollisuus tai oikeus antaa taikka oikeus saada muutoin salassa pidettävää tietoa, sillä julkisen tiedon antaminen tai saaminen perustuu julkisuuslain säännöksiin.

3.2 Tiedustelumenetelmin saadun tiedon antaminen hybridiuhkan torjumiseksi

Tässä luvussa keskitytään tiedustelumenetelmien käyttämisen avulla saatujen tiedustelutietojen ja niiden sisältämien henkilötietojen antamiseen toiselle viranomaiselle tai muulle taholle tiedusteluviranomaisten eli suojelupoliisin ja Puolustusvoimien toimesta. Tarkoituksena on selvittää, millaisia mahdollisuuksia tiedusteluviranomaisilla on tiedustelutiedon antamiseen erityisesti oma-aloitteisesti ja mitkä säännökset säätävät tietojen antamisesta. Julkisuuslain 4.1 §:n mukaan laissa tarkoitettuja viranomaisia ovat valtion hallintoviranomaiset sekä muut valtion virastot ja laitokset, joten julkisuuslakia noudatetaan yleislakina myös tiedusteluviranomaisten toiminnassa. Lähtökohtaisesti tiedustelutietoa sisältävät asiakirjat eivät ole julkisia julkisuuslain 24.1 §:n 9–10 kohtien nojalla. Tiedustelutietojen salassapito määräytyy sen perusteella, mitä tieto koskee ja onko tiedot saatu siviilitiedustelun vai sotilastiedustelun menetelmillä[209]. Salassapitoa tukee myös se, että useimmiten tiedusteluasiakirjat sisältävät tietoa, jota koskee julkisuuslain 22.1 §:ssä säädetty vaitiolovelvollisuus[210]. Kuten muidenkin salassa pidettävien asiakirjojen antamisessa, niin myös tiedustelutietoa sisältävien asiakirjojen antamisessa tulee noudattaa tarpeellisuus- tai välttämättömyysvaatimusta, joten tieto salassa pidettävästä tiedusteluasiakirjasta voidaan antaa vain, jos se on tarpeen toisen viranomaisen tai tietoa antavan viranomaisen tehtävien hoitamiseksi tai se on välttämätöntä muun kuin viranomaisen tehtävien suorittamiseksi[211].

[209] Mäenpää, 2023, s. 825.
[210] Lohse & Viitanen, 2019, s. 81.
[211] LiVL 26/2018 vp, s. 4; HaVM 30/2018 vp, s. 82. Ks. myös mm. PeVL 31/2017 vp, s. 2, jossa taustaa välttämättömyyden ja tarpeellisuuden arvioinnista.

Julkisuuslain 24.1 § 9 kohdan mukaan suojelupoliisin ja muiden viranomaisten valtion turvallisuuden ylläpitämistä koskevat asiakirjat ovat salassa pidettäviä, jollei ole ilmeistä, että tiedon antaminen näistä asiakirjoista ei vaaranna valtion turvallisuutta. Samoin myös sotilastiedustelua ja muutoin merkityksellistä maanpuolustukseen liittyvää tietoa sisältävät asiakirjat ovat salassa pidettäviä, jollei ole ilmeistä, että tiedon antaminen niistä ei vaaranna tai vahingoita maanpuolustuksen etua (JulkL 24.1 § 10 kohta). Kuitenkin, jos tiedustelutieto koskee Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön, asiakirjat ovat salassa pidettäviä vain, jos tiedon antaminen niistä aiheuttaisi vahinkoa tai haittaa Suomen kansainvälisille suhteille tai yhteistyölle (JulkL 24.1 § 2 kohta). Muutoin kansainvälisiä suhteita koskevat tiedot ovat julkisia eli tietoihin kohdistuu julkisuusolettama. Jos siviilitiedustelulla saadut tiedot koskevat PolL 5a luvun 5 §:ssä mainittua tiedonhankintaa, jonka aikana ilmenee tietoja PolL 5 luvun 3 §:ssä säädetyistä rikoksista, ja joiden estämiseksi tai selvittämiseksi tiedusteluviranomainen saa jatkaa tiedonhankintaansa, ovat tiedustelumenetelmällä hankitut tiedot ehdottoman salassapidon piirissä (JulkL 24.1 § 4 kohta). Näitä PolL 5 luvun 3 §:ssä tarkoitettuja rikoksia ovat esimerkiksi vakoilu, laiton tiedustelutoiminta ja terrorismiin liittyvä toiminta, jotka voivat olla myös hybridivaikuttamisen keinoja. Näin ollen tiedustelutietoa sisältävät asiakirjat ovat lähtökohtaisesti salassa pidettäviä, eikä niistä pääsääntöisesti voi antaa tietoa pyynnöstä taikka oma-aloitteisesti, vaan tietojen antaminen määräytyy tapauskohtaisesti.

Kuitenkin valtion turvallisuutta koskevien tiedustelutietoja sisältävien asiakirjojen antamisessa viranomaiselle on jätetty laissa harkintavaltaa ja viranomainen voi tapauskohtaisen harkintansa mukaan myös antaa tällaista tietoa, jos se katsoo, ettei tiedon antaminen vaaranna valtion turvallisuutta tai maanpuolustuksen etua[212]. Julkisuuslain 24.1 § 9–10 kohtien säännöksiin sisältyy siis salassapito-olettamaan perustuvat vahinkoedellytyslausekkeet, joiden mukaan kyseiset asiakirjat ja tiedot ovat yleensä salassa pidettäviä, ja niistä voidaan antaa tietoa vain, jos siitä ei ilmeisesti aiheudu haitallisia vaikutuksia

[212] Mäenpää, 2023, s. 825.

tässä tapauksessa valtion turvallisuudelle tai maanpuolustukselle[213]. Seuraavassa ratkaisussaan korkein hallinto-oikeus on punninnut asianosaisen oikeutta saada itseään koskeva tieto suhteessa valtion turvallisuutta koskevaan yleiseen etuun.

> KHO 2020:4: Tapauksessa oli kyse julkisuuslain 24.1 §:n 9 kohdan mukaisten valtion turvallisuuden ylläpitämistä koskevien asiakirjojen käyttämisestä suojelupoliisin Maahanmuuttovirastolle antaman lausunnon taustamateriaalina A:n turvapaikkahakemukseen liittyen. A oli pyytänyt saada tiedon suojelupoliisin lausunnon perusteluosiosta ja siihen käytetystä taustamateriaalista. A:lla oli tapauksessa julkisuuslain 11.1 §:n mukainen lähtökohtainen asianosaisen tiedonsaantioikeus myös suojelupoliisin asiakirjoista, mutta kyseinen oikeus ei ole ehdoton ja sitä voidaan rajoittaa JulkL 11.2 §:ssä säädettyjen perusteiden mukaisesti. Perusteluosion ja lausunnon taustamateriaalina käytettyjen asiakirjojen todettiin sisältävän sellaisia tietoja, joiden antaminen olisi ollut vastoin JulkL 11.2 §:n 1 kohdassa tarkoitettua valtion turvallisuutta koskevaa erittäin tärkeää yleistä etua, joten A ei ollut oikeutettu saamaan tietoa asiakirjoista.[214]

Kun viranomainen käyttää harkintavaltaansa salassa pidettävän tiedon antamisessa, voi se pyytää tietopyynnön tehnyttä tahoa perustelemaan pyyntöään[215]. Lisäksi harkinnassa tulee huomioida hallintolain 6 §:ssä määritellyt hallinnon oikeusperiaatteet, joiden mukaan harkintavallan käytön on oltava oikeasuhtaista, tasapuolista ja puolueetonta ja harkintavaltaa saa käyttää vain lain mukaan hyväksyttäviin tarkoituksiin ja siinä on huomioitava yksilön perustellut odotukset[216]. Salassapidosta poikkeamisessa tulee huomioida myös perustuslailla suojatut perusoikeudet, kuten julkisuusperiaate (PL 12.2 §), yksityiselämän suoja (PL 10 §) ja tieteen vapaus (16.3 §)[217].

Koska julkisuuslaissa on säädetty tiedusteluviranomaisten tiedustelutietoa sisältävien asiakirjojen olevan pääsääntöisesti salassa pidettäviä, tulee tämän tutkimuksen kannalta kyseeseen sellaiset erityislainsäädännön säännökset, joilla salassapidosta voidaan poiketa ja tietoa antaa toiselle viranomaiselle myös tiedustelutiedosta. Seuraavaksi käsittelen näiden erityissäännösten pohjalta tiedustelutiedon antamista toiselle viranomaiselle pääasiassa tiedustelulakien kautta. Tässä luvussa keskitytään siis tiedustelumenetelmin

---

[213] Mäenpää, 2017, s. 390.
[214] KHO 2020:4.
[215] Kulla, 2012, s. 382.
[216] Mäenpää, 2020a, s. 245.
[217] Mäenpää, 2020a, s. 246.

hankittujen tiedustelutietojen ja niiden sisältämien henkilötietojen luovuttamiseen toiselle viranomaiselle tai muulle taholle. Tarkoituksenani on selvittää, voivatko tiedusteluviranomaiset antaa oma-aloitteisesti tiedustelutietoa toisille viranomaisille tai muille tahoille. Pyrin jäsentelemään ne säännökset, jotka mahdollistavat tiedusteluviranomaisten oma-aloitteisen tietojen antamisen erityisesti silloin, kun tiedustelulla on saatu selville hybridiuhkaan viittaavaa tietoa.

3.2.1 Tiedustelutiedon antaminen toimivaltaiselle viranomaiselle

Tiedustelutietojen luovuttamisesta toiselle viranomaiselle on säädettävä erikseen lain tasolla, kuten muistakin salassa pidettävien tietojen luovuttamisesta[218]. Tiedustelutietojen luovuttamisesta säädetään tiedustelulakien ohella tietosuojalaissa, julkisuuslaissa, henkilötietojen käsittelystä poliisitoimessa annetussa laissa, henkilötietojen käsittelystä Puolustusvoimissa annetussa laissa, SKRTL:ssä ja kansainvälisistä tietoturvavelvoitteista annetussa laissa (588/2004)[219]. Kuten aiemmin on todettu, julkisuuslaissa siviili- ja sotilastiedustelua koskevat asiakirjat ja tiedot yhdessä muiden maanpuolustusta koskevien tietojen kanssa on katsottu lähtökohtaisesti salassa pidettäviksi (JulkL 24.1 § 9–10 kohta). Tiedustelun keinoilla hankitun tiedon antamiseen pätee myös julkisuuslain 26 §:n yleiset perusteet sekä 27–30 §:n erityiset perusteet, joiden nojalla salassa pidettävää tietoa voi antaa. Seuraavaksi käsittelen niitä sotilastiedustelulakiin, siviilitiedustelua koskevaan poliisilain 5 a lukuun, tietoliikennetiedustelusta siviilitiedustelussa annettuun lakiin ja muuhun erityislainsäädäntöön sisältyviä säännöksiä, joiden nojalla muutoin salassa pidettävän tiedustelumenetelmin hankitun tiedon voi antaa toiselle viranomaiselle.

Sotilastiedustelulla hankitaan tietoa pääasiassa Suomen turvallisuusympäristön kehityksestä, johon ensi sijassa liittyy vieraiden valtioiden asevoimien toimintaan liittyvät kysy-

[218] HE 203/2017 vp, s. 122.
[219] HE 203/2017 vp, s. 122.

mykset ja niistä tiedon hankkiminen maanpuolustuksen ja kansallisen turvallisuuden turvaamiseksi [220]. Sotilastiedustelulla pyritään myös havaitsemaan turvallisuusympäristöömme kohdistuvia uhkia ja muodostamaan uhkatoimista tilannekuva, jonka pohjalta viranomaiset voivat ryhtyä tarvittaviin torjuntatoimiin. Siviilitiedustelu sen sijaan keskittyy hankkimaan tietoa kaikkein vakavimmista kansallista turvallisuutta uhkaavista ilmiöistä ja hankkeista, joista saatuja tietoja hyödyntämällä suojelupoliisi ryhtyy itse toimenpiteisiin kansallisen turvallisuuden suojaamiseksi tai jakaa tietoa muille kansallista turvallisuutta suojaaville viranomaisille ja ylimmälle valtiojohdolle[221]. Samalla suojelupoliisin tehtävänä on poliisin hallinnosta annetun lain (110/1992, muutettu lailla 583/2019) 10.1 §:n mukaan havaita, estää ja paljastaa valtio- tai yhteiskuntajärjestystä tai sisäistä tai ulkoista turvallisuutta uhkaavia toimintoja, hankkeita ja rikoksia sekä ylläpitää ja kehittää yleistä valmiutta tällaisen uhkaavan toiminnan havaitsemiseksi ja estämiseksi. Tehtävillä korostetaan suojelupoliisin tiedonhankinnallista ja tiedustelullista tehtävää kansallisen turvallisuuden suojaamiseksi[222].

Kuten aiemmin luvussa 2.2.2 olen kuvannut, tiedustelulaeissa on toimivaltasäännöksiä tiedustelun kohdistamisesta erilaisiin hybridiuhkia synnyttäviin vieraan valtion tai muun toimijan toimiin, joilla pyritään horjuttamaan kansallista turvallisuutta tai maanpuolustusta. Kun toimivaltuudet tiedustelun kohdistamiseen hybridivaikuttamisen osana esiintyvään toimintaan ovat olemassa, onkin tärkeää selvittää, milloin tiedustelulla hankittu tieto voidaan antaa eteenpäin toiselle viranomaiselle sen tehtävien hoitamiseksi.

Sotilastiedustelun yhtenä päätehtävänä on tuottaa tietoa Suomen turvallisuusympäristössä tapahtuvista muutoksista ja vakavimmista turvallisuusuhista, jotka kohdistuvat ensi sijassa maanpuolustukseen[223]. Puolustusvoimien tehtävänä on toimittaa sotilastiedustelulla hankittu tieto turvallisuusympäristön muutoksista ylimmän valtiojohdon käyttöön

[220] HE 203/2017 vp, s. 135.
[221] HE 202/2017 vp, s. 168-169.
[222] HE 202/2017 vp, s. 263.
[223] HE 203/2017 vp, s. 178.

ja tällä tavalla tukea valtiojohdon päätöksentekoa (SotTiedL 3 §). Pääasiassa sotilastiedustelulla saatua tietoa luovutetaan siis ylimmän valtiojohdon käyttöön, joiden lisäksi lailla säädetyt tietyt viranomaiset voivat esittää tietopyynnön sotilastiedustelun kohteista. SotTiedL 14 §:n mukaan tietopyynnön SotTiedL 13.1 §:ssä tarkoitetuista TP-UTVA:n valmistelemista sotilastiedustelun kohteiden painopisteistä voivat tehdä tasavallan presidentti, valtioneuvoston kanslia, ulkoministeriö ja puolustusministeriö. Edellä mainittuja tilanteita koskee laissa säädetyt tiedonantovelvollisuudet, eikä kyse ole varsinaisesti oma-aloitteisesta tietojen antamisesta, vaikkakin Puolustusvoimien pääesikunta luovuttaa tiedustelutiedot ylimmälle valtiojohdolle osana lakisääteisiä tehtäviään eikä niitä näin ollen tarvitse erikseen pyytää. Muiden ulko- ja turvallisuuspoliittisesti merkittävien viranomaisten tapauksessa tiedonanto sen sijaan perustuu pääesikunnalle tehtävään tietopyyntöön.

Ylin valtiojohto tekee sotilastiedustelulla hankitun tiedon pohjalta päätöksen ryhtyä toimiin esimerkiksi sotilaallisen tai muun vakavan turvallisuusuhkan torjumiseksi tai estämiseksi. Tällöin ylin valtiojohto tiedottaa toimiin ryhtymisestä asianmukaisia viranomaisia, jolloin tiedustelutieto suodattuu muille viranomaisille ylimmän valtiojohdon kautta, eikä tietoa näin ollen luovuta toiselle viranomaiselle itse sotilastiedusteluviranomainen[224]. Lähtökohtaisesti tiedustelutieto kulkeutuisi siis ylimmän valtiojohdon kautta tarvittaville tahoille, kuten viranomaisille tai yrityksille. Kuitenkin sotilastiedustelulakiin ja lakiin tietoliikennetiedustelusta siviilitiedustelussa on säädetty poikkeussäännökset haitallisia tietokoneohjelmia koskien, jolloin tiedusteluviranomaiset saavat luovuttaa salassapitosäännösten estämättä tietoliikennetiedustelulla saadut haitallista tietokoneohjelmaa koskevat tiedot viranomaiselle, yritykselle ja yhteisölle, jos se on tarpeen sotilaallisen maanpuolustuksen, kansallisen turvallisuuden suojaamisen tai yrityksen tai yhteisön etujen turvaamisen kannalta (SotTiedL 74 § ja TtStL 16 §). Kyse voisi olla myös muun muassa hybridivaikuttamisesta, jonka osana hyödynnettäisiin haitallisen tietokoneohjelman levittämistä pyrkimyksenä lamaannuttaa yhteiskunnan kriittisiä toimintoja.

[224] HE 203/2017 vp, s. 179.

Säännöksessä tarkoitettu tietojen antaminen olisi sallittua edellä mainituissa tilanteissa, eikä kyseessä siten olisi tietojenantovelvollisuus vaan pikemminkin tiedonanto-oikeus. Näin ollen tietojen antaminen perustuisi aina tapauskohtaiseen harkintaan, jolloin maanpuolustukseen tai kansalliseen turvallisuuteen liittyvät syyt voivat myös estää tietojen antamisen, vaikka se olisikin yrityksen tai yhteisön etujen turvaamiseksi tarpeen[225]. Lähtökohtaisesti tämänkaltainen tietojen antaminen toimivaltaiselle viranomaiselle tapahtuisi silloin, kun tiedolla olisi laajempi yhteiskunnallinen merkitys ja tiedon levittäminen sujuisi paremmin toimivaltaisten viranomaisten toimesta kuin sotilastiedusteluviranomaisen välityksellä[226]. Kyseessä olisi oma-aloitteinen tietojen antaminen, kun tiedon antaminen perustuu tiedusteluviranomaisen omaan harkintaan.

Keskeistä tiedustelutoiminnassa on yhteistyö muiden viranomaisten ja kansainvälisten toimijoiden kanssa, mikä juontaa juurensa hallintolain 10 §:ssä säädetystä yleisestä viranomaisten välisestä yhteistyöstä. Yhteistyön merkitys tiedustelutoiminnassa korostuu jatkuvasti koko yhteiskunnan kattavan kokonaisturvallisuusajattelun vahvistuessa niin kansallisesti, EU:n tasolla kuin kansainvälisestikin. Sotilastiedusteluviranomaisen yhteistyö on laajimmillaan siviilitiedustelua suorittavan suojelupoliisin kanssa, koska sotilaalliset tai kansalliseen turvallisuuteen kohdistuvat uhkat eivät aina ole selkeästi erotettavissa pelkästään siviili- tai sotilastiedustelun kohteiksi, ainakaan alkuvaiheessa. Tiedustelulakeja säädettäessä on korostettu tiedusteluviranomaisten keskinäistä yhteistyötä ja edellytetty niiden välistä saumatonta tietojenvaihtoa, jotta uhkien kehittymistä voidaan arvioida jatkuvasti ja tarvittaessa siirtää tiedustelutehtävä toiselle tiedusteluviranomaiselle, jos kohde kuuluukin enemmän tämän tehtäväkenttään[227]. Tiedusteluviranomaisten yhteistyössä korostuu saumaton tiedustelutietojen vaihto, millä varmistetaan riittävä tiedonsaanti toistensa toteuttamasta tiedustelutoiminnasta, jotta toinen tiedusteluviranomainen ei omalla toiminnallaan tietämättään estäisi tai vaarantaisi toisen suorittamaan tiedusteluoperaatiota[228].

---

[225] HE 203/2017 vp, s. 297
[226] HE 203/2017 vp, s. 297.
[227] HE 203/2017 vp, s. 212.
[228] HE 202/2017 vp, s. 226; HE 203/2017 vp, s. 212.

Tiedusteluviranomaisten välisestä yhteistyöstä on säädetty samansisältöisin säännöksin SotTiedL 17 §:ssä ja PolL 5a luvun 54 §:ssä, joiden mukaan tiedusteluviranomaisten on toimittava yhteistyössä heidän tarkoitustenmukaisten tehtäviensä hoitamiseksi sekä annettava toisilleen tehtävien kannalta tarpeellisia tietoja salassapitovaatimusten estämättä. Säännökset täsmentävät kyseisten viranomaisten keskinäistä yhteistyötä ja säätävät myös tiedusteluviranomaisten välisestä tietojenvaihdosta erityisesti salassa pidettävän tiedon osalta, johon viranomaisyhteistyön yleissäännös HL 10 § ei anna yleistä oikeutta. Säännökset koskevat kuitenkin vain tiedustelutiedon jakamista ja henkilötietojen luovuttamisesta säädetään erikseen henkilötietojen käsittelystä Puolustusvoimissa annetussa laissa (332/2019) sekä henkilötietojen käsittelystä poliisitoimessa annetussa laissa (616/2019).

Muiden viranomaisten kanssa tehtävästä yhteistyöstä säädetään sotilastiedustelun osalta SotTiedL 18 §:ssä ja siviilitiedustelun osalta PolL 5a luvun 55 §:ssä, joiden mukaan tiedusteluviranomaiset voivat luovuttaa muille viranomaisille salassapitosäännösten estämättä muita tietoja kuin henkilötietoja oman tiedustelutehtävänsä suorittamiseksi, jos se on tarpeen sotilastiedustelussa maanpuolustuksen tai kansallisen turvallisuuden vuoksi (SotTiedL 18.1 §) ja siviilitiedustelussa kansallisen turvallisuuden suojaamiseksi (PolL 5a:55.2). Viranomaisille luovutettavan tiedustelutiedon osalta lakiin on siis kirjattu tarpeellisuusvaatimus, minkä vuoksi tietojen luovuttamisen toiselle viranomaiselle tulee olla tarpeellista, jotta tiedusteluviranomainen voi suorittaa omat tehtävänsä kansallisen turvallisuuden tai maanpuolustuksen suojaamiseksi. Tiedot voidaan luovuttaa myös, jos se on tarpeellista toiselle viranomaiselle kuuluvien kansallista turvallisuutta tai maanpuolustusta suojaavien tehtävien suorittamiseksi, koska kyse on tiedusteluviranomaiselle säädetyn kansallisen turvallisuuden tai maanpuolustuksen turvaamistehtävän toteuttamisesta[229].

[229] HE 202/2017 vp, s. 227; HE 203/2017 vp, s. 213. Ks. tarpeellisuusvaatimuksesta myös perustuslakivaliokunnan lausuntokäytäntö mm. PeVL 31/2017 vp & PeVL 1/2015 vp ja siinä viitatut lausunnot.

Lisäksi muun tiedustelutiedon kuin henkilötiedon voi luovuttaa salassapitosäännösten estämättä yritykselle tai yhteisölle tiedustelutehtävän toteuttamiseksi, jos se on välttämätöntä Puolustusvoimien toiminnan tai kansallisen turvallisuuden suojaamiseksi (SotTiedL 18.2 §) tai siviilitiedustelussa kansallisen turvallisuuden suojaamiseksi (PolL 5a:55.3). Lisäksi sotilastiedusteluviranomainen voi tehtävänsä suorittamiseksi luovuttaa salassapitosäännösten estämättä yrityksille tai yhteisöille haittaohjelmaan liittyvän tunnistamistiedon, jotta tiedustelumenetelmiä tai järjestelmiä voidaan kehittää (SotTiedL 18.2 §). Näissä SotTiedL 18.2 §:n ja PolL 5a luvun 55.3 §:n tilanteissa tiedusteluviranomainen tekisi harkinnan tietojen luovuttamisesta omaan tehtäväkenttäänsä liittyen ja tietojen luovuttamisen tulisi olla tehtävien suorittamiseksi välttämätöntä[230]. Tiedustelutietojen antaminen voi tulla kyseeseen oma-aloitteisena tai pyynnöstä tapahtuvana tietojen antamisena, mutta tiedon luovuttamisen tulee kuitenkin aina liittyä tiedusteluviranomaisten lakisääteisten tehtävien toteuttamiseen.

Sotilastiedustelulakia koskevassa hallituksen esityksessä on korostettu myös tiedon saamisen kohteena olevien yritysten roolin arviointia maanpuolustuksessa tai yhteiskunnan elintärkeiden toimintojen tuottamisessa, jolloin niille voitaisiin antaa tietoa myös yritysvakoilun tai niiden turvallisuuden ehkäisemiseksi kansallisen turvallisuuden suojaamisen nojalla[231]. Tällä on esityksessä tarkoitettu esimerkiksi tilanteita, joissa tiedustelutiedon antaminen yksityisille yhteisöille olisi tarpeen vakavien uhkien torjunnan aloittamiseksi tai merkittävien taloudellisten tappioiden estämiseksi[232]. Kyse voisi olla hybridivaikuttamisesta, jonka osana hyödynnettäisiin tietoverkkoympäristössä tapahtuvaa vakoilua useimmiten rajat ylittävästi ja tällä tavalla pyrittäisiin hankkimaan tietoa, jonka avulla voitaisiin vahingoittaa kohdevaltion turvallisuutta ja etuja. Tällaisen toiminnan havaitseminen ja estäminen ovat olennainen osa myös siviilitiedusteluviranomaisen kansallisen turvallisuuden turvaamistehtävää. Hallintovaliokunta on mietinnössään korostanut tarvetta erilaisten yritysten, yhteisöjen ja yksityisten roolien ja toiminnan tunnistamiselle,

[230] HE 202/2017 vp, s. 227; HE 203/2017 vp, s. 213.
[231] HE 203/2017 vp, s. 213.
[232] HE 203/2017 vp, s. 162.

sillä viestintäpalveluita voivat tuottaa myös muut kuin perinteiset teleyritykset, mitä ei ole vielä riittävästi tiedonantosäännöksissä tunnistettu[233].

Kansallisten toimijoiden välisen yhteistyön lisäksi kansainvälisellä yhteistyöllä on keskeinen rooli tiedustelutoiminnassa, vaikka tiedustelutoiminnan ensisijaisena tarkoituksena onkin edistää kansallisen edun parantamista. Kansainvälinen yhteistyö kattaa muun muassa tiedustelutietojen vaihtamisen muiden maiden tiedustelu- ja turvallisuusviranomaisten tai vastaavien tahojen kanssa. Sotilastiedustelun kohteena olevat uhkat ovat usein kansainvälisiä, jolloin ulkomaalaisilla tiedustelu- ja turvallisuuspalveluilla on mahdollista saada niistä Suomen kansallisen turvallisuuden kannalta merkittävää tietoa[234]. Näin ollen onkin katsottu tarpeelliseksi, että sotilastiedusteluviranomainen voi Suomen kansallisten etujen mukaisesti vaihtaa muita tiedustelutietoja kuin henkilötietoja näiden tahojen kanssa salassapitosäännösten estämättä, jos se on tarpeellista sotilastiedusteluviranomaisen omiin tehtäviin liittyen tai kansallisen turvallisuuden suojaamiseksi (SotTiedL 20.1, 1 §). Tämä tarkoittaa, että sotilastiedusteluviranomainen voi luovuttaa hankkimiaan tietoja ulkomaiselle tiedusteluviranomaiselle, jos se on Suomen edun kannalta tarpeellista esimerkiksi sotilaallisten uhkien tai kriisien tunnistamiseksi[235].

Myös siviilitiedusteluviranomainen voi luovuttaa muita kuin henkilötietoja kansainvälisen yhteistyön nojalla, jos tietojen luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi ja se on kansallisen edun mukaista (PolL 5a:57.4). Kansallisen edun piiriin on katsottu kuuluvan muun muassa Suomen taloudelliset tai poliittiset suhteet toisen valtion kanssa sekä kansainvälisen tiedustelutiedon turvaamista koskevat tiedot[236]. Lähtökohtaisesti tiedustelutietojen antaminen kansainvälisessä yhteistyössä on oma-aloitteista tietojen antamista, koska vain suojelupoliisi tai sotilastiedusteluviranomainen voi tehdä intressipunnintaa tietojen antamisen tarpeellisuudesta kansallisen turvallisuuden, maanpuolustuksen ja kansallisen edun turvaamisen välillä. Erityisesti sotilastiedustelun,

[233] HaVM 35/2022 vp, s. 9.
[234] HE 203/2017 vp, s. 214.
[235] HE 203/2017 vp, s. 214.
[236] HE 202/2017 vp, s. 229.

mutta myös siviilitiedustelun osalta on tarpeen tehdä muutoksia kansainvälistä yhteistyötä koskeviin säännöksiin, jotta tiedustelutietoa voidaan antaa ja vaihtaa myös Naton kanssa, sillä nykyiset säännökset koskevat lähtökohtaisesti tietojen antamista muiden valtioiden tiedustelu- ja turvallisuusviranomaisille.

Lisäksi sotilastiedusteluviranomainen voi saada tehtäviinsä liittyviä tietoja ulkomaisilta tiedustelu- tai turvallisuusviranomaisilta esimerkiksi kansainvälisiin uhkiin tai henkilötiedusteluun liittyen, ja näiden tietojen pohjalta Puolustusvoimat voisivat käynnistää oman ulkomaan henkilötiedustelun tai muun tiedustelutoimivaltuuden käytön[237]. Kansainvälisen yhteistyön kautta saatuun tiedustelutietoon liittyy aina epävarmuustekijöitä ja tietojen luotettavuus ja paikkansapitävyys tulee varmistaa sotilastiedusteluviranomaisen toimesta esimerkiksi käynnistämällä oma tiedusteluoperaatio erityisesti henkilöihin liittyvissä tiedoissa[238]. Vastaavasti myös siviilitiedusteluviranomainen voi saada kansainväliseen tiedusteluyhteistyöhön kuuluvan tiedonvaihdon kautta tehtäviinsä liittyvää tietoa. Kansainvälisessä tietojenvaihdossa kyse voisi olla esimerkiksi kansainvälisen järjestäytyneen rikollisryhmän toiminnasta, josta tiedon vaihtaminen edistäisi kansallisen turvallisuuden toteutumista esimerkiksi silloin, jos toiminta on sellaista, jolla pyritään vaikuttamaan yhteiskunnalliseen päätöksentekoon tai soluttautumaan valtiorakenteisiin. Tällöin kyse voisi olla myös hybridiuhasta, jos rikollisryhmä toimii esimerkiksi kolmannen valtion tai muun toimijan ohjauksen alaisena ja toiminnan pyrkimyksenä on muitakin keinoja hyödyntämällä vaikuttaa kohdevaltioon.

Kansainväliseen vakiintuneeseen tapaoikeuteen perustuen ulkomaisilta tiedusteluviranomaisilta saatuihin tietoihin kohdistuu luovutuskielto kolmansille osapuolille ilman luovuttajamaan suostumusta[239]. Korkein hallinto-oikeus on päätöksissään 2012:8, 2010:31

[237] HE 203/2017 vp, s. 214.
[238] HE 203/2017 vp, s. 214.
[239] KHO 2012:8, s. 5–6.

ja 2003:77 punninnut kansainvälisen tiedonvaihdon kautta saatujen tietojen luottamuksellisuutta ja julkisuusperiaatteen toteutumista erityisesti suojelupoliisin kansallisen turvallisuuden ylläpitämiseen liittyvien tehtävien kannalta.

> KHO 2012:8, KHO 2010:31 ja KHO 2003:77: Tapauksissa oli kyse kansainvälisen yhteistyön kautta luottamuksellisesti saatuihin tiedustelutietoihin kohdistuvista asiakirjapyynnöistä, jotka suojelupoliisi oli hylännyt vedoten muun muassa julkisuuslain 24.1 §:n 9 kohdan mukaiseen salassapitoon valtion turvallisuuden vaarantumisen nojalla. Kaikissa tapauksissa korkein hallinto-oikeus oli katsonut, että asiakirjojen sisällön perusteella ei voitu varmistua siitä, että tietojen antaminen ei vaarantaisi valtion turvallisuutta, joten tiedot olivat salassa pidettäviä eikä niistä voinut antaa tietoa. KHO oli päätöksissään myös ottanut kantaa suojelupoliisin tietojen saamistapaan ja korosti, että kansainvälisen tiedustelutietojenvaihdon kautta saatuja tietoja koskee luottamuksellisuus ja tällaisten tietojen julkistaminen voisi vaikuttaa kielteisesti ulkomaisten tiedustelu- ja turvallisuusviranomaisten halukkuuteen luovuttaa jatkossa luottamuksellista tiedustelutietoa suojelupoliisille, mikä saattaisi heikentää suojelupoliisin kansallisen turvallisuuden suojaamiseen liittyvien tehtävien hoitamista.[240]

Edellä SotTiedL 18 § ja 20 § sekä PolL 5a luvun 55 § ja 57 § tarkoitetuissa tilanteissa tietojen luovuttaminen perustuu tiedusteluviranomaisen oikeuteen luovuttaa toisille viranomaisille tai yrityksille ja yhteisöille muutoin salassa pidettävää tiedustelutietoa, joka ei sisällä henkilötietoja. Kyseessä on siis tiedonanto-oikeus eikä tiedusteluviranomainen ole velvollinen antamaan tietoa toiselle viranomaiselle, vaan se päättää tietojen antamisesta oman harkintansa puitteissa. Yrityksille ja yhteisöille luovutettaessa painottuu erityisesti tietojen luovuttamisen välttämättömyys kansallisen turvallisuuden ja maanpuolustuksen kannalta ja kansainvälisille toimijoille luovutettaessa tulee huomioida edellisten lisäksi Suomen kansallinen etu. Kyseessä on siis ensisijaisesti tiedusteluviranomaisen oma-aloitteinen tietojenanto-oikeus, jolloin tiedusteluviranomainen päättää tiedustelumenetelmin hankkimaansa tietoa analysoituaan tiedon antamisesta toiselle viranomaiselle, yksityisen sektorin toimijalle tai kansainväliselle toimijalle. Tosin erityisesti tiedon antaminen toiselle viranomaiselle voi perustua myös viranomaisen pyyntöön, joten tietojen antaminen ei aina ole oma-aloitteista.

---

[240] KHO 2012:8; KHO 2010:31; KHO 2003:77.

Sen sijaan tiedusteluviranomaisten keskinäisestä yhteistyöstä säätävät säännökset SotTiedL 17 § ja PolL 5a luvun 54 § velvoittavat niin suojelupoliisin kuin Puolustusvoimien tiedusteluviranomaisenkin antamaan toisilleen tarpeellisia tietoja, joiden osalta kyseessä on tiedonantovelvollisuus. Tiedusteluviranomaisten välinen tietojen antaminen on lähtökohtaisesti oma-aloitteista tietojen antamista, koska tiedusteluviranomaisilla on velvollisuus pitää toisensa ajan tasalla toiminnastaan, mutta tietoja voidaan antaa myös pyynnöstä.

3.2.2 Tiedustelutietojen antaminen rikostorjuntaviranomaisille

Tiedustelulakien esitöissä on korostettu, että tiedustelutoimivaltuuksilla ei ole merkittävää roolia rikosten ennalta ehkäisemisessä ja selvittämisessä, vaan tiedustelulla pyritään havainnoimaan nimenomaan maanpuolustukseen ja kansalliseen turvallisuuteen kohdistuvia uhkia[241]. Kuitenkin siviili- ja sotilastiedustelussa voidaan joskus saada tietoa rikoksista tai vaaratilanteista, joista ilmoittamisella on mahdollista estää tilanteen kehittyminen vakavan rikoksen tekemiseen. Tällaisista tiedoista ilmoittaminen on vastoin tiedustelutoiminnan käyttötarkoitusta, koska tiedustelulla ei pyritä estämään tai selvittämään rikoksia. Sen vuoksi tiedustelulakeihin on otettu poikkeussäännökset, jotka koskevat tiedustelutiedon luovuttamista rikostorjuntaviranomaisille ja näin ollen ne poikkeavat tiedustelutiedon käyttötarkoitussidonnaisuudesta. Näitä säännöksiä kutsutaan palomuurisäännöksiksi, ja ne asettavat edellytykset sille, milloin tiedustelutietoja pitää, saa tai ei saa luovuttaa rikostorjuntaviranomaisille[242]. Palomuurisäännökset on kirjattu poliisilain 5a luvun 44 §:ään ja sotilastiedustelulain 79–80 §:iin. Lisäksi se, mitä säädetään PolL 5a luvun 44 §:ssä pätee myös siviilitiedustelun tietoliikennetiedustelulla saadun tiedon luovuttamiseen rikostorjuntaan (TtStL 17 §).

[241] HE 202/2017 vp, s. 149 ja 263; HE 203/2017 vp, s. 302.
[242] Valtioneuvosto, 2021b, s. 23.

Palomuurisäännökset asettavat tietyn kynnyksen rikosta koskevien tietojen ilmoittamiselle, jotta tiedustelumenetelmällä saadun tiedon käyttötarkoitussidonnaisuus säilyisi vain tiedustelutehtävän hoitamiseen eikä tiedustelumenetelmiä käytettäisi yleisesti rikosten selvittämiseen tai estämiseen[243]. Vaikka hybridivaikuttamisessa pyritään usein hyödyntämään sinänsä laillisia keinoja, voi toiminta olla rikollista esimerkiksi silloin, kun sen osana suunnitellaan tai jopa toteutetaan terrori-isku kohdevaltiossa. Myös hybridivaikuttamisessa hyödynnettävä kybervaikuttaminen voi olla luonteeltaan rikollista tai muuttua rikolliseksi, kun esimerkiksi yhteiskunnan kriittisten toimijoiden tietojärjestelmiä häiritään palvelunestohyökkäyksillä tai niihin kohdistetaan datavahingonteko ja tekojen tavoitteena on esimerkiksi häiritä yhteiskunnan elintärkeitä toimintoja tai pyrkiä vaikuttamaan kohdevaltion päätöksentekoon[244].

Palomuurisääntelyn mukaan tiedusteluviranomaisen on ilmoitettava ilman aiheetonta viivytystä keskusrikospoliisille, jos tiedustelun myötä ilmenee, että voidaan olettaa tehdyksi rikos, josta säädetty ankarin rangaistus on vähintään 6 vuotta vankeutta (SotTiedL 79.1 § ja PolL 5a:44.1). Kyseessä on siis ilmoitusvelvollisuus, josta voidaan poiketa vain siirtämällä tiedon antamista myöhemmäksi pääesikunnan tiedustelupäällikön tai suojelupoliisin päällikön päätöksellä laissa mainituista välttämättömistä syistä enintään vuodeksi kerrallaan (SotTiedL 79.1 § ja PolL 5a:44.1).

Tiedusteluviranomainen sen sijaan saa ilmoittaa tehdystä rikoksesta keskusrikospoliisille, jos ilmoituksella olisi oletettavasti erittäin tärkeä merkitys sellaisen rikoksen selvittämiselle, josta säädetty ankarin rangaistus on vähintään 3 vuotta vankeutta (SotTiedL 79.2 § ja PolL 5a:44.1). Kyseessä on siis viranomaisen ilmoitusoikeus ja tiedusteluviranomaisen harkintaan perustuva oma-aloitteinen tietojen antaminen. Säännökset pitävät samalla kuitenkin sisällään tietojen luovutuskiellon sellaisista tehdyistä rikoksista, joista säädetty ankarin rangaistus alittaisi kolme vuotta, jolloin tällaista rikosta koskevat tiedot tulisi aina

[243] HE 202/2017vp, s. 214; HE 203/2017 vp, s. 303.
[244] Tieto- ja viestintärikoksista säädetään rikoslain 38 luvussa ja datavanhingonteoista rikoslain 35 luvun 3 a-c §:ssä.

jättää antamatta[245]. Tällöin tiedusteluviranomaiselle jää harkintavalta ilmoittaa tehdyistä rikoksista, joista säädetty vankeusrangaistus jää vähintään kolmen vuoden ja enintään kuuden vuoden seuraamusuhan väliin[246].

Kun tiedusteluviranomainen harkitsee ilmoituksen tekemistä tai siirtämistä myöhemmäksi, tulee sen arvioida ilmoituksen merkitystä kansalliseen turvallisuuden suojaamiseen sekä rikoksen selvittämisen merkitystä yleisen ja yksityisen edun kannalta (PolL 5a:44.3) sekä sotilastiedustelussa edellä mainittujen lisäksi ilmoituksen merkitystä maanpuolustuksen kannalta (SotTiedL 79.3 §). Harkinnanvaraa liittyy siis SotTiedL 79.1 §:ssä ja PolL 5a luvun 44.1 §:ssä tarkoitettuun ilmoituksen teon siirtämiseen myöhemmäksi oletettavasti tehdyistä rikoksista, joista on säädetty rangaistukseksi vähintään kuusi vuotta vankeutta tai sellaisista SotTiedL 79.2 §:ssä ja PolL 5a luvun 44.1 §:ssä tarkoitetuista tehdyistä rikoksista ilmoittamiseen, joista on säädetty rangaistukseksi vähintään kolme vuotta, mutta kuitenkin enintään kuusi vuotta vankeutta. Näistä ilmoittamista tulee harkita arvioimalla SotTiedL 79.3 §:ssä ja PolL 5a luvun 44.3 §:ssä esitettyjä arviointiperusteita.

Tehtyjen rikosten ohella tiedusteluviranomaisille on säädetty velvollisuus ilmoittaa viipymättä toimivaltaiselle viranomaiselle, jos se saa tiedustelulla selville, että on tekeillä rikos, josta on säädetty ankarimmaksi rangaistukseksi vähintään kuusi vuotta vankeutta ja rikos voitaisiin vielä estää (SotTiedL 80.1 § ja PolL 5a:44.2). Tiedustelulla saatua tietoa voidaan luovuttaa toimivaltaiselle viranomaiselle myös sellaisen rikoksen estämiseksi, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta (SotTiedL 80.2 § ja PolL 5a:44.2). Tämän rangaistusuhan alittavista rikoksista saadut tiedot tulisi aina jättää tiedusteluviranomaisen toimesta luovuttamatta tiedon luovutuskiellosta johtuen. Näin ollen tiedusteluviranomaiselle jää harkintavalta ilmoittaa sellaisista tekeillä olevista rikoksista, joista on säädetty ankarimmaksi rangaistukseksi vähintään 2 vuotta, mutta kui-

[245] HE 202/2017 vp, s. 216; HE 203/2017 vp, s. 305.
[246] HE 202/2017 vp, s. 216; HE 203/2017 vp, 305.

tenkin enintään 6 vuotta vankeutta. Tiedustelulakien esitöiden mukaan säännöksissä tarkoitettu tieto voisi liittyä rikosten estämisen ohella muun muassa rikoksen paljastamiseen tai esitutkinnan aloittamisen selvittämiseen[247]. Tiedon luovuttamista tulee harkita samoin perustein kuin jo tehdyistä rikoksista ilmoittamisestakin on säädetty painottaen erityisesti henkeen ja terveyteen kohdistuvien rikosten uhkaa[248].

Tekeillä olevista rikoksista ilmoittamisessa on kyse oma-aloitteisesta tietojen antamisesta, mutta ilmoitusvelvollisuus tekeillä olevasta ns. ylitörkeästä rikoksesta, josta voi ankarimmillaan saada rangaistukseksi vähintään kuusi vuotta vankeutta, on sidottu viipymättä tehtävään ilmoitukseen, jolloin ilmoittamiselle ei jätetä harkinnanvaraa. Kuitenkin SotTiedL 80.3 §:ssä on mainittu myös ylitörkeästä rikoksesta tehtävän ilmoituksen sisältävän harkintavaltaa, mutta lain esitöissä tällaista ei mainita, vaan harkinnanvaraa sisältyy vain ilmoittamiseen tekeillä olevasta rikoksesta, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta.

Erityisesti tekeillä olevista rikoksista ilmoittaminen voi auttaa hybridiuhkien torjumisessa, jos tiedusteluviranomainen saa tietoonsa sellaisia tekeillä olevia rikoksia tai hankkeita, jotka viittaavat liittyvän hybridivaikuttamiseen tai -sodankäyntiin. Käsitykseni mukaan tällaisia palomuurisääntelyn täyttäviä tekeillä olevia rikoksia voisivat olla muun muassa törkeät datavahingonteot (RL 35:3 b), törkeä tietoliikenteen häirintä (RL 38:6) ja törkeä tietojärjestelmän häirintä (RL 38:7 b). Näin ollen käsitykseni mukaan esimerkiksi tekeillä olevasta lievästä datavahingonteosta (RL 35:3) tai lievästä tietoliikenteen häirinnästä (RL 38:7) ei voisi ilmoittaa rikostorjuntaviranomaiselle, mutta sen sijaan tekeillä olevasta törkeästä datavahingonteosta tai törkeästä tietoliikenteen häirinnästä voitaisiin ilmoittaa rikostorjuntaviranomaiselle palomuurisäännösten nojalla, koska niistä säädetty ankarin rangaistus on vähintään 2 vuotta vankeutta. Lisäksi esimerkiksi RL 34 a luvun 2 §:n mukaisen terroristisessa tarkoituksessa tehtävän rikoksen valmistelusta olisi ilmoitettava ri-

[247] HE 202/2017 vp, s 217; HE 203/2017 vp, s. 307.
[248] HE 202/2017 vp, s. 217; HE 203/2017 vp, s. 307.

kostorjuntaviranomaiselle. Rikostorjuntaviranomaisille voitaisiin antaa tietoa myös sellaisista tekeillä olevista rikoksista, joissa edellä kuvatut törkeä datavahingonteko sekä törkeä tietoliikenteen ja tietojärjestelmän häirintä tehtäisiin terroristisessa tarkoituksessa siten, että ne aiheuttaisivat vakavaa vahinkoa valtiolle tai kansainväliselle järjestölle (RL 34 a luvun 1.1 §:n 4 kohta). Silloin kun tällaiset teot ovat osa hybridivaikuttamista tai -sodankäyntiä, voidaan oma-aloitteisella tietojen antamisella mahdollisesti torjua kyseiset hybridiuhkan osatekijät.

Lisäksi tiedusteluviranomaisilla on aina oikeus antaa tiedustelulla saatua tietoa henkilön syyttömyyden tueksi ja hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran taikka huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi (SotTiedL 79.4 § ja 80.4 § sekä PolL 5a:44.4). Tiedon antaminen syyttömyyttä tukevan selvityksen osaksi voi perustua esimerkiksi rikoksesta epäillyn pyyntöön taikka tiedusteluviranomaisen oma-aloitteiseen tiedon ilmoittamiseen lähinnä tilanteissa, joissa tiedusteluviranomainen on saanut tiedon sen kohteena olevaa tai ollutta henkilöä koskevasta esitutkinnan tai rikostorjunnan aloittamisesta[249]. Säännöksissä tarkoitetun vaaran tai vahingon ei sen sijaan tarvitse lakien esitöiden mukaan liittyä rikokseen vaan kyse voi olla vaikkapa onnettomuuden estämisestä tai johonkin yritykseen kohdistuvan tietoverkkohyökkäyksen estämisestä[250]. Näin ollen tietoja voidaan antaa toimivaltaisen viranomaisen lisäksi myös yrityksille, yhteisöille tai yksityisille henkilöille, jos se on tarpeen momentissa lueteltujen vaarojen tai vahinkojen estämiseksi[251].

Edellä tarkoitettua merkittävää vaaraa tai vahinkoa koskeva ilmoitus voidaan tehdä toimivaltaisen viranomaisen lisäksi myös yksityiselle henkilölle, yritykselle tai yhteisölle, jos se on tarpeen kyseisen vaaran tai vahingon estämiseksi[252]. Kyseeseen voisi tulla esimerkiksi jo edellisessä luvussa 3.2.1 mainittu yrityksen, yhteisön tai yksityisen taloudellisen

[249] HE 203/2017 vp, s. 307.
[250] HE 202/2017 vp, s. 218; HE 203/2017 vp, s. 307.
[251] HE 202/2017 vp, s. 2018; HE 203/2017 vp, s. 307.
[252] HE 202/2017 vp, s. 218; HE 203/2017 vp, s. 308.

vahingon estäminen luovutetun tiedustelutiedon avulla. Näidenkin tietojen luovuttaminen on tiedusteluviranomaisen oikeus, jolloin ilmoituksen tekemiseen jää harkinnanvaraa säädettyjen arviointikriteerien mukaisesti. Sotilastiedustelulaissa on jätetty pääesikunnan tiedustelupäällikölle toimivalta päättää harkinnanvaraisten tietojen ilmoittamisesta ja luovuttamisesta rikostorjuntaviranomaiselle (SotTiedL 79.6 § ja 80.6 §), kun siviilitiedustelua koskevassa poliisilain 5a luvun 44 §:ssä ei ole erillistä toimivaltasäännöstä harkinnanvaraisten tietojen antamisesta päättämiseen. Näissä tilanteissa tietojen antaminen on oma-aloitteista.

Tiedusteluvalvontavaltuutettu ja Eduskunnan oikeusasiamies ovat esittäneet kantansa tiedustelulakien palomuurisääntelyn tulkinnasta. Tiedusteluvalvontavaltuutettu katsoo, että tiedusteluviranomaiset voisivat ilmoittaa palomuurisäännösten estämättä tiedustelumenetelmin saadun rikokseen liittyvän tiedon esitutkintaviranomaisille silloin, kun kyse on tiedustelutoiminnan käyttötarkoitukseen kuuluvien kansallista turvallisuutta uhkaavien tai sotilaallista maanpuolustusta vaarantavien rikosten estämisestä, paljastamisesta tai selvittämisestä. Tällaisia rikoksia olisivat esimerkiksi sellaiset maanpetos-, valtiopetos- ja terrorismirikokset, joista säädetty ankarin rangaistus on alle kolme vuotta vankeutta, kuten tuottamuksellinen turvallisuussalaisuuden paljastaminen tai maanpetoksellinen yhteydenpito.[253] Eduskunnan oikeusasiamies on sen sijaan tulkinnut palomuurisääntelyä siten, että se velvoittaa tiedusteluviranomaisia kaikenlaisia rikoksia koskevien tiedustelutietojen luovuttamisessa, jolloin tiedustelumenetelmän käytön aikana ilmeneviin rikoksiin voidaan reagoida ainoastaan palomuurisäännösten osoittamissa rajoissa[254].

Virvotieto -hankkeen yhteydessä toteutetuissa haastatteluissa suojelupoliisista nousi esiin epäselvyyttä EOA:n palomuurisääntelyn tulkinnasta siltä osin, että katsooko EOA palomuurin sääntelevän kaikkien tietojen luovuttamista rikostorjuntaviranomaisille vai sääntelekö se ainoastaan konkreettisia rikoksia koskevan tiedon luovuttamista. Tässä

[253] Tiedusteluvalvontavaltuutettu, 2020, s. 25.
[254] EOAK/289/2021, s. 28.

yhteydessä Supo toi esiin hybridiuhkien torjumisen haastavuuden, koska hybridiuhkaa ei välttämättä luokitella rikokseksi, jolloin nykyisen tulkintakäytännön valossa on epäselvää, voiko Supo antaa tällaisesta hybridiuhkasta tiedustelumenetelmin saamansa tiedon toiselle viranomaiselle palomuurisäännöksistä välittämättä vai ei.[255] Tiedusteluvalvontavaltuutetun kertomuksesta voi tulkita, että tällaisesta ei-rikolliseksi katsottavasta hybridiuhkaan viittaavasta toiminnasta voitaisiin antaa tieto toimivaltaisille viranomaisille, kun kyseessä on kansallisen turvallisuuden tai maanpuolustuksen suojaaminen. Eduskunnan oikeusasiamiehen tulkinnasta sen sijaan voisi tulkita, että tällaisen tiedon antaminen ei olisi mahdollista palomuurisääntelystä johtuen. Kuitenkin aiemmassa luvussa 3.2.1 on kuvattu niitä tiedustelulakien säännöksiä, joiden nojalla tiedon antaminen erilaisista hybridivaikuttamisessa tai -sodankäynnissä käytettävistä keinoista on mahdollista, kun kyseessä ei ole vielä ainakaan tiedonhankintavaiheessa rikos tai rikokseen tähtäävä toiminta. Näin ollen voidaan tulkita, että palomuurisääntely koskisi nimenomaan rikoksista saatuja tiedustelutietoja ja muuta hybridiuhkaan viittaavaa tiedustelutietoa voisi antaa muille tahoille lain sen salliessa, koska hybridiuhkaan viittaavan tiedon jakaminen on myös tiedustelutoiminnan käyttötarkoituksen mukaista.

3.2.3 Tiedustelumenetelmin saatujen henkilötietojen antaminen

Edellä mainitut säännökset sääntelevät tiedustelumenetelmin saadun tiedon antamisesta toisille viranomaisille tai muille tahoille, mutta ne eivät sisällä henkilötietojen luovuttamiseen liittyviä tilanteita. Henkilötietojen luovuttamista rajoittaa useat säännökset, joista keskeisin on perustuslain 10 §:ssä säädetty yksityiselämän suoja ja siihen osittain kuuluva henkilötietojen suoja. Euroopan unionin yleinen tietosuoja-asetus (Neuvoston asetus 2016/679/EU) ja sitä täydentävä tietosuojalaki (1050/2018) säätävät yleisistä rajoituksista ja perusteista henkilötietojen käsittelylle Euroopan unionin alueella ja näillä

[255] Kurvinen ja muut, 2023, s. 159.

säännöksillä pyritään suojaamaan luonnollisten henkilöiden yksityisyyttä koskevien tietojen käsittelyä sekä muita tietoja, jotka voidaan liittää luonnolliseen henkilöön[256].

Kuitenkaan tietosuoja-asetusta ja tietosuojalakia ei sovelleta kansallista turvallisuutta koskeviin toimiin, vaan silloin henkilötietojen käsittelyssä noudatetaan henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain (1054/2018, myöhemmin rikosasioiden tietosuojalaki) sekä muiden erityislakien säännöksiä[257]. Kuitenkin rikosasioiden tietosuojalain 2.1 §:n mukaan lain säännöksiä ei sovelleta, jos muussa laissa on poikkeavia säännöksiä. Tiedustelutoiminnassa saatujen henkilötietojen käsittelystä ja luovuttamisesta säädetään erikseen laeissa henkilötietojen käsittelystä Puolustusvoimissa (332/2019, myöhemmin Puolustusvoimien henkilötietolaki) sekä henkilötietojen käsittelystä poliisitoimessa (616/2019, myöhemmin poliisin henkilötietolaki). Näiden lakien säännökset tulevat siis ensisijaisesti sovellettaviksi tiedustelutoiminnassa, minkä lisäksi rikosasioiden tietosuojalain säännökset voivat tulla sovellettaviksi joissain tilanteissa, jos tiedustelulla on saatu tietoa rikoksesta tai sen valmistelusta ja siitä ilmoittaminen täyttää edellä kuvattujen palomuurisäännösten vaatimukset. Näiden lisäksi julkisuuslaki säätää henkilötietojen luovuttamisesta viranomaisen henkilötietorekisteristä, eikä siihen sovellu EU:n yleinen tietosuoja-asetus tai kansallinen tietosuojalaki.

Poliisin henkilötietolain 7 luku käsittelee suojelupoliisin henkilötietojen käsittelyä ja säätää näin ollen suojelupoliisin henkilötietojen luovuttamisesta myös tiedustelutoiminnassa. Puolustusvoimien henkilötietolain 4 luvussa taas käsitellään yhteisesti henkilötietojen luovuttamista ja tiedonsaantioikeuksia ja siitä löytyy säännökset myös sotilastiedustelulla saatujen henkilötietojen luovuttamiseen. Puolustusvoimien henkilötietolain 32 § säätää tiedustelutiedon antamisesta toiselle valtiolle tai kansainväliselle järjestölle. Lain 32.1 §:n mukaan sotilastiedustelutehtävässä hankittuja henkilötietoja saa luovuttaa

[256] Korpisaari, Pitkänen & Warma-Lehtinen, 2018, s. 1.
[257] Krakau ja Haapalehto, 2020, s. 193.

toiselle valtiolle tai kansainväliselle järjestölle, jos se on välttämätöntä kansallisen turvallisuuden varmistamiseksi. Tietojen luovuttamisessa tulee kuitenkin huomioida henkilötietoja vastaanottavan valtion ihmisoikeustilanne, luovutuksen merkitys Suomen kansainvälisille suhteille sekä Suomea sitovat kansainväliset sopimukset ja velvoitteet (32.1§). Lisäksi Puolustusvoimat saa luovuttaa tietoja kyseisen lain 29 §:ssä mainituille viranomaisille ja julkista tehtävää hoitaville yhteisöille niiden laissa säädettyjen tehtävien suorittamiseksi sekä 30.1 §:n mukaan, jos tietojen antaminen on välttämätöntä yksittäisen tehtävän hoitamiseksi. Henkilötietoja voi antaa myös Puolustusvoimien henkilötietolain 30.2 §:n 3 kohdan mukaisesti viranomaisille sekä yhteisöille ja yksityisille henkilöille, jos tietojen antaminen on välttämätöntä hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran taikka huomattavan ympäristö-, omaisuus tai varallisuusvahingon estämiseksi.

Suojelupoliisi sen sijaan saa luovuttaa henkilötietoja toiselle viranomaiselle tai julkista tehtävää hoitavalle yhteisölle omien tehtäviensä suorittamiseksi (poliisin henkilötietolain 50.1 §). Lisäksi suojelupoliisi saa luovuttaa henkilötietoja muille poliisiyksiköille lain 13 §:n käsittelytarkoituksiin sekä muulle viranomaiselle tai julkista tehtävää hoitavalle yhteisölle 4 luvussa tarkoitettuihin käsittelytarkoituksiin (50.2 §). Lisäksi suojelupoliisi saa yksittäistapauksessa luovuttaa henkilötietoja yksityiselle yhteisölle tai henkilölle, jos se on välttämätöntä suojelupoliisin tehtävän suorittamiseksi ja siihen on painava syy (50.4 §). Poliisin henkilötietolain 51 § sääntelee henkilötietojen luovuttamisesta kansainvälisille toimijoille ja säännöksen mukaan suojelupoliisi saa luovuttaa henkilötietoja ulkomaan turvallisuus- ja tiedustelupalvelulle sekä viranomaiselle, jonka tehtäviin kuuluu muun muassa kansallisen turvallisuuden suojaaminen, jos luovuttaminen on välttämätöntä suojelupoliisin tehtävän suorittamiseksi tai mainittujen ulkomaan viranomaisten tehtävien suorittamiseksi (51 § 1–2 mom.). Kuten Puolustusvoimien henkilötietolain säännöksissä henkilötietojen luovuttamisesta ulkomaille, myös suojelupoliisin tulee huomioida henkilötietoja vastaanottavan valtion ihmisoikeustilanne, luovutuksen merkitys Suomen kansainvälisille suhteille sekä Suomea sitovat kansainväliset sopimukset ja muut velvoitteet (51.4 §).

Lähtökohtaisesti henkilötietojen antaminen Puolustusvoimien tai suojelupoliisin toimesta perustuukin Puolustusvoimien ja poliisin henkilötietolaeissa välttämättömyysvaatimukseen, jonka mukaan tietojen luovutuksen tulee olla välttämätöntä joko kansallisen tai ulkomaan viranomaisen tai muun tahon tehtävien suorittamiseksi. Lisäksi henkilötietojen antaminen on viranomaisten tiedonanto-oikeus, eivätkä säännökset näin ollen velvoita tiedusteluviranomaisia antamaan henkilötietoja muille tahoille, vaan kyse on tapauskohtaisesta harkinnasta. Näillä toimenpiteillä voidaan varmistua henkilötietojen asianmukaisesta käytöstä ja luonnollisten henkilöiden perus- ja ihmisoikeuksien turvaamisesta. Seuraavaksi pohdinkin vielä yksityisyyden suojan toteutumista tiedustelutoiminnassa ja viranomaisten välistä tietojen antamista suhteessa viranomaisten työn tehokkuuteen erityisesti kansallista turvallisuutta uhkaavien toimintojen selvittämisessä ja torjumisessa. Tarkoitus on pohtia, voidaanko tiedustelutoiminnalla saatu tieto antaa toiselle viranomaiselle viranomaisten työn tehokkuudella perustellen ja miten yksityisyyden suoja turvataan tiedustelutoiminnassa.

4 Yksityisyyden suoja tiedustelutoiminnassa ja viranomaisten työn tuloksellisuus

Jokaisen yksityiselämä on turvattu perustuslain 10 §:n sekä myös Euroopan ihmisoikeussopimuksen (SopS 18–19/1990) 8 artiklan nojalla. Lailla turvattu yksityiselämän suoja on keskeisin osa yksityisyyden suojaa, mutta Neuvosen mukaan yksityisyyden suojaan katsotaan kuuluvan myös muita elementtejä, kuten muut perus- ja ihmisoikeuksilla turvattavat yksilön oikeudet[258]. Näin ollen yksityisyyden suoja voidaan katsoa henkilön yksityistä piiriä koskevaksi yleiskäsitteeksi[259]. Yksi yksityisyyden ja yksityiselämän suojan osa-alueista on henkilötietojen suoja, jonka keskeisenä tarkoituksena on taata yksityiselämän suoja ja yksilön oikeusturva niin henkilötietojen käsittelyssä ja käyttämisessä kuin niiden luovuttamisessa[260]. Merkittävää sääntelyn kannalta on kuitenkin erottaa henkilötietojen suoja yksityisyyden suojasta omaksi perusoikeudekseen, sillä henkilötietojen suojaan kuuluu yksityiselämää koskevien tietojen lisäksi muita henkilöön liitettävissä olevia tietoja ja näiden tietojen kokoamiseen ja käsittelyyn liittyviä seikkoja[261]. Henkilötietojen suojasta säädetään perusoikeutena kansallisesti samassa yhteydessä yksityiselämän suojan kanssa perustuslain 10.1 §:ssä sekä EU:n perusoikeuskirjan[262] 8 artiklassa. Henkilötietojen käsittelystä henkilöiden oikeusturvaa ja yksityisyyttä kunnioittavalla tavalla säädetään erikseen EU:n yleisessä tietosuoja-asetuksessa (Neuvoston asetus 2016/679/EU) ja sitä täydentävässä kansallisessa tietosuojalaissa (1050/2018).

Tietosuoja-asetus ja tietosuojalaki sääntelevät henkilötietojen käsittelystä tilanteissa, joissa tiedoista muodostuu tai on tarkoitus muodostaa rekisteri tai sen osa[263]. Vaikka viranomaisen toiminnassa henkilötietoja tallennetaan useinkin erilaisiin rekistereihin, on tietosuojalain 28 §:ssä säädetty, että viranomaisen henkilörekisteristä tiedon saamiseen

[258] Neuvonen, 2014, s. 37.
[259] HE 198/2017 vp, s. 4.
[260] Mäenpää, 2023, s. 643.
[261] Korpisaari, Pitkänen & Warma-Lehtinen, 2018, s. 15.
[262] EUVL N:o C 202, 7.6.2016, s. 395.
[263] Mäenpää, 2023, s. 643.

ja muuhun henkilötietojen luovuttamiseen sovelletaan julkisuuslain säännöksiä. Näin ollen viranomaisen asiakirjoihin sisältyvien henkilötietojen luovuttaminen määräytyy julkisuuslain mukaisesti. Kuitenkin henkilötietojen käsittelystä ja luovuttamisesta on säädetty eri viranomaisten toimintaa sääntelevissä erityislaeissa, kuten aiemmassa luvussa 3.2.3 on kuvattu tiedusteluviranomaisten osalta.

Tämän luvun tarkoituksena on kuvata, miten yksityisyyden suoja on huomioitu tiedustelutoimivaltuuksia säädettäessä. Käytän tässä tutkielmassa käsitteenä yksityisyyden suojaa, koska se käsittää muiden perusoikeuksien lisäksi niin yksityiselämän sekä henkilötietojen suojan, vaikkakin tämän luvun kannalta merkittävin säännös on yksityiselämän suojaa sääntelevä perustuslain 10 §. Aion pohtia, miten tiedustelumenetelmien käyttämisessä huomioidaan yksityisyyden suoja ja milloin kansallisen turvallisuuden tai maanpuolustuksen nojalla voidaan hankkia tietoa yksityisyyden suojaan kuuluvista asioista. Lisäksi pohdin hyvän hallinnon oikeusperiaatteenakin esiintyvän viranomaisten välisen yhteistyön merkitystä tehokkuuden näkökulmasta, sillä viranomaisyhteistyön tarkoituksena on tehostaa hallinnon toimivuutta ja näin ollen viranomaisten työskentelyä[264].

Vaikka tehokkuutta ei ole viety lainsäädäntöön erilliseksi hyvän hallinnon periaatteeksi, voidaan viranomaisilta edellyttää tehokkuutta eurooppalaisen hallintotavan valkoisen kirjan (Komission tiedonanto (EY) 2001/428)[265] nojalla. Valkoisessa kirjassa on yhtenä hyvän hallintotavan periaatteena mainittu tehokkuus, joka koskee kaikkia jäsenvaltioiden hallinnon tasoja niin keskus-, alue- kuin paikallishallinnossakin. Hallintotoiminnan tehokas hoitaminen edellyttää muun muassa ripeää ja tuloksellista toimintaa[266]. Käytännössä kyse on siis toiminnan ja tehtävien hoitamisesta taloudellisesti kustannustehokkaasti niin, että viranomaisen resursseja hyödynnetään oikeasuhtaisesti. Tehokkuutta voidaan edis-

[264] Kulla, 2012, s. 122.
[265] EYVL N:o C 287, 12.10.2001, s. 7.
[266] Mäenpää, 2020b, s. 36

tää hallintolain 10 §:n mukaisella viranomaisten välisellä yhteistyöllä erityisesti hallintotoiminnassa, mutta onko viranomaisten välinen tietojen vaihtaminen keino viranomaistoiminnan tehokkuuden ja tuloksellisuuden toteuttamiseksi.

4.1 Yksityisyyden suojan huomioiminen tiedustelutoiminnassa

Kuten aiemmissa luvuissa on käynyt ilmi, tiedustelumenetelmin saadut tiedot ovat lähtökohtaisesti salassa pidettäviä ja salassapito kohdistuu myös tiedustelutietojen sisältämiin henkilötietoihin, joskin niiden salassapitoa sääntelevät eri säännökset. Näin pyritään turvaamaan luonnollisten henkilöiden yksityisyyden suojaa, sillä sen turvaaminen edellyttää tehokasta salassapitosääntelyä yksityisyyttä ja yksityiselämää koskevista tiedoista[267]. Kuitenkin EIS 8 artiklan 2 kohdassa on säädetty, että viranomaiset saavat puuttua yksityiselämän suojaan, jos se on välttämätöntä muun muassa kansallisen turvallisuuden vuoksi tai epäjärjestyksen tai rikollisuuden estämiseksi. Tiedusteluviranomaisten toiminnassa on kyse kansallisen turvallisuuden suojaamisesta, minkä vuoksi tiedustelulakien säätämisen yhteydessä perustuslain 10 §:ään lisättiin uusi neljäs momentti, jonka mukaan lailla voidaan säätää välttämättömistä rajoituksista luottamuksellisen viestin suojaan muun muassa tiedon hankkimiseksi sotilaallisesta toiminnasta tai muusta kansallista turvallisuutta vakavasti uhkaavasta toiminnasta (PL 10.4 §).

PL 10.4 §:n tilanteissa puututaan yksityisyyden suojaan kuuluvan luottamuksellisen viestin suojaan, josta on säädetty tarkemmin säännöksen 2 momentissa, EIS 8 artiklassa sekä EU:n perusoikeuskirjan 7 artiklassa, jonka mukaan jokaisen yksityis- ja perhe-elämää, kotia ja viestejä tulee kunnioittaa. PL 10.2 § säädetään erityisesti luottamuksellisen viestin salaisuudesta ja salaisuuden loukkaamattomuudesta. Perus- ja ihmisoikeudet ovat pe-

[267] Mäenpää, 2023, s. 626.

rustavanlaatuisia oikeuksia, joihin puuttuminen on mahdollista vain laintasoisen säännöksen nojalla ja kyseisten oikeuksien keskeistä sisältöä kunnioittaen[268]. Lisäksi EU:n perusoikeuskirjan 52 artiklan 1 kohdan mukaan perusoikeuksien rajoitusten tulee olla välttämättömiä ja vastata unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojata muiden henkilöiden oikeuksia ja vapauksia. Siksi luottamuksellisen viestin suojaan puuttumisesta tiedon hankkimiseksi sotilaallisesta toiminnasta tai muusta kansallista turvallisuutta uhkaavasta toiminnasta tuli säätää erillinen säännös perustuslakiin.

Kansallisen turvallisuuden käsite oli jo ennen PL 10.4 § säätämistä käytössä lainsäädännössä ja erityisesti Euroopan unionin oikeusjärjestyksessä ja kansainvälisissä ihmisoikeussopimuksissa myös ihmisoikeuksien rajoittamisen perusteena, muun muassa viestin salaisuuden kohdalla. Euroopan ihmisoikeustuomioistuimen ratkaisukäytännössä kansallista turvallisuutta vaarantavan toiminnan määrittely kuuluu valtioiden varsin laajaan harkintamarginaaliin, mikä käy ilmi seuraavista tapauksista. EIT:n tapauksessa Al-Nashif v. Bulgaria (20.6.2002) EIT katsoi, että lain ennakoitavuuden vaatimus ei velvoita valtiota säätämään laissa kaikenlaisesta käyttäytymisestä, joka voisi johtaa yksilön karkottamiseen kansallisen turvallisuuden perusteella, sillä kansallisen turvallisuuden uhat ovat luonteeltaan ennalta-arvaamattomia ja vaikeasti määriteltävissä[269]. Myös EIT:n tapauksessa Kennedy v. Yhdistynyt Kuningaskunta (18.5.2010) EIT katsoi aiempaan käytäntöönsä perustuen, että samanlaiset näkökohdat koskevat kansallisen turvallisuuden termin käyttöä myös salaisen valvonnan yhteydessä, minkä vuoksi laissa ei tarvitse luetella yksityiskohtaisesti kaikkia kansallista turvallisuutta mahdollisesti uhkaavia toimia[270].

Perustuslain 10.4 §:ssä kansallinen turvallisuus on mielletty myös melko laajana käsitteenä, jolla tarkoitetaan valtion oikeudenkäyttöpiirissä olevien ihmisten kollektiivista tur-

[268] HE 198/2017 vp, s. 24.
[269] EIT tapaus Nashif v. Bulgaria, 20.6.2002.
[270] EIT tapaus Kennedy v. Yhdistynyt Kuningaskunta, 18.5.2010.

vallisuutta ja sitä vakavasti uhkaavalla toiminnalla suuren ja ennalta-arvaamattoman ihmisjoukon henkeä ja terveyttä uhkaavaa toimintaa[271]. Samalla pykälässä säädetään tiedon hankkimisesta valtioon kohdistuvasta sotilaallisesta toiminnasta, jolla tarkoitetaan sekä valtiollisten että ei-valtiollisten, sotilaallisesti järjestäytyneiden tai sotavoimaa käyttävien joukkojen toimintaa taikka sotilaallisiin voimakeinoihin liittyvää toimintaa[272]. Säännöksen tarkoittama niin sotilaallinen kuin kansallista turvallisuutta uhkaava toiminta voisi käytännön toimenpiteisiin edetessään olla rikos, mutta johon ei ainakaan vielä tiedonhankintavaiheessa voida kohdistaa konkreettista ja yksilöityä rikosepäilyä[273].

Tiedon hankkiminen edellä kuvatuista toimista ei saa olla yleistä, kohdentamatonta ja kaiken kattavaa tietoliikenteen seurantaa, sillä EIT ja EUT ovat ratkaisukäytännössään painottaneet, että tiedonhankinnalla ei saisi puuttua rajoittamattomasti luottamuksellisen viestin salaisuuden suojaan. Esimerkiksi EIT tapauksessa Zakharov v. Venäjä (4.12.2015) tuomioistuin katsoi, että lainsäädäntö salaisesta tietojen hankkimisesta yksilön luottamuksellisesta viestinnästä ei ollut riittävän ennakoitavissa eikä se tarjonnut tiedonhankinnan kohteelle asianmukaista oikeusturvaa, sillä laissa oli säädetty viranomaisille rajoittamaton toimivalta määritellä edellytykset luottamuksellisen viestin suojaan puuttumiselle. EIT katsoi, että lainsäädäntö oli vastoin Euroopan ihmisoikeussopimuksen vaatimuksia ja asetti päätöksellään salaisia tiedonhankintamenetelmiä koskevalle lainsäädännölle vähimmäisvaatimukset, jotka estäisivät viranomaisten mielivaltaisen puuttumisen luottamuksellisen viestin suojaan. EIT totesi, että lainsäädännössä tulisi olla riittävät ja tehokkaat takeet viranomaisten mielivaltaisuuden ja väärinkäytön riskiä vastaan ja laissa tulisi olla selkeät rajoitukset perus- ja ihmisoikeuksiin puuttumiselle, jotta se olisi mahdollista vain siltä osin, kuin se on välttämätöntä demokraattisen yhteiskunnan turvaamiselle.[274]

[271] HE 198/2017 vp, s. 35.
[272] HE 198/2017 vp, s. 34.
[273] HE 198/2017 vp, s. 34–35.
[274] EIT tapaus Zakharov v. Venäjä, 4.12.2015.

Perustuslain 10.4 § säädettäessä on päädytty tulokseen, että riittävistä oikeusturva- ja valvontamenettelyistä momentin tilanteisiin kohdistettavassa tiedonhankinnassa säädetään tavallisen lain nojalla, eikä niitä koskevia säännöksiä ole otettu perustuslakiin[275]. Kuitenkin menettelyistä säädettävissä laeissa tulee huomioida perusoikeuksien yleiset rajoitusperusteet, kun tiedustelumenetelmillä puututaan perustuslain 10 §:n turvaamaan yksityiselämän suojaan. Tiedustelumenetelmien käytön edellytyksistä säädetään poliisilain 5a luvun 4 §:ssä ja sotilastiedustelulain 12 §:ssä, mutta erityisesti luottamuksellisen viestin salaisuuden suojaan puuttumisesta esimerkiksi telekuuntelun tai muun vastaavan menetelmän avulla säädetään erikseen siten, että sellaisen menetelmän käyttö edellyttää tuomioistuimen päätöstä, jolla annetaan lupa telekuunteluun tai muuhun vastaavaan tietojenhankintamenetelmään enintään kuudeksi kuukaudeksi kerrallaan (PolL 5a:6 ja SotTiedL 36 §). Tuomioistuinmenettelyn tarkoituksena on estää tiedustelutoimivaltuuksien väärinkäyttö ja sitä kautta osaltaan turvata yksilön riittävän oikeusturvan toteutuminen[276].

Tiedustelulakien esitöissä on luottamuksellisen viestin suojan lisäksi pohdittu muita yksityiselämän ja näin ollen yksityisyyden suojan piiriin kuuluviin oikeuksiin puuttumista tiedustelumenetelmin. Perustuslain 10 §:ssä on turvattu luottamuksellisen viestin salaisuuden suojan lisäksi viestin tunnistamistiedot, jokaisen kotirauha ja henkilötietojen suoja, jota olen käsitellyt jo aiemmin luvussa 3.2.3, joten en palaa siihen enää tässä yhteydessä. Viestin lähettäjän ja vastaanottajan tunnistamistietojen salaisuuden suojaaminen nousi perustuslakivaliokunnan tulkintakeskusteluun vasta EUT:n Digital Rights Ireland -asiassa antaman ratkaisun myötä, missä EUT katsoi, että kerättyjen tunnistamistietojen kokonaisuus muun muassa sähköisen viestinnän lähteestä ja kohteesta sekä matkaviestintälaitteesta voi mahdollistaa hyvin tarkkojen päätelmien tekemisen tietoja koskevan henkilön yksityiselämästä, kuten vakituisista tai väliaikaisista oleskelupaikoista, liikkumisesta ja sosiaalisista suhteista[277].

---

[275] HE 198/2017 vp, s. 38.
[276] HE 198/2017 vp, s. 39.
[277] C-293/12 ja C-594/12, Digital Rights Ireland ym., EU:C:2014:238.

Perustuslakivaliokunta arvioi tuomion myötä sähköisten viestien tunnistamistietoja uudelleen luottamuksellisen viestin suojan näkökulmasta, ja totesi tunnistamistietojen keräämisen ja kokoamisen mahdollisuuden olevan ongelmallista yksityiselämän suojan näkökulmasta siinä määrin, että luottamuksellisen viestin suojan rajoittamisessa tulee kiinnittää huomiota yleisesti rajoitusten merkittävyyteen[278]. Tämä tarkoittaa, että jatkossa luottamuksellisen viestin suojaan puuttumista tulee arvioida niin viestin sisällön salaisuuden kuin viestin tunnistetietojen salaisuuden näkökulmasta siten, mitä niihin puuttuminen kokonaisuudessaan merkitsee henkilön yksityisyyden suojalle. Kumpikin ulottuvuus on huomioitu tiedustelulaeissa ja siksi myös viestin tunnistamistietoihin kohdistuvaan televalvontaan vaaditaan lähtökohtaisesti tuomioistuimen lupa (SotTiedL 38.1 § ja PolL 5a:7).

Edellä kuvattuihin luottamuksellisen viestin salaisuuden ja viestin tunnistamistietojen salaisuuden suojaan saa siis puuttua tiedustelumenetelmin, jos se on välttämätöntä tiedon hankkimiseksi sotilaallisesta toiminnasta tai kansallista turvallisuutta vakavasti uhkaavasta toiminnasta[279]. Kuitenkin yksityiselämän piiriin kuuluvaan kotirauhaan ei lähtökohtaisesti saa siviili- tai sotilastiedustelulla puuttua, mikä tarkoittaa sitä, että tiedustelumenetelmiä ei saa kohdistaa vakituiseen asumiseen käytettävään tilaan, pois lukien peitetoiminnan ja valeoston tilanteet silloin, kun asuntoon sisäänkäynti ja siellä oleskelu tapahtuu asuntoa käyttävän aktiivisella myötävaikutuksella[280]. Tästä voidaan tulkita, että kotirauhan suojalla on painava merkitys yksityiselämän suojaamisessa, sillä siihen ei ole säädetty rajoituksia ainakaan tiedustelutoimivaltuuksia säädettäessä, mikä tarkoittaa, ettei siihen voida puuttua tiedustelumenetelmillä edes vakavimmissa uhkatilanteissa.

[278] PeVL 18/2014 vp, s. 6.
[279] Yksityiselämän suojan kannalta merkityksellisiä tiedustelumenetelmiä ovat suunnitelmallinen tarkkailu, peitelty tiedonhankinta, tekninen kuuntelu, tekninen katselu, peitetoiminta, valeosto ja paikkatiedustelu. (HE 202/2017 vp, s. 271.)
[280] HE 202/2017 vp, s. 271; HE 203/2017 vp, s. 351.

Tämä on merkityksellistä tämän tutkimuksen kannalta siltä osin, että usein hybridivaikuttamisesta tietoa hankittaessa kyseeseen ei tule peitetoiminnan tai valeoston menetelmät, jolloin kotirauhan piirissä tapahtuvasta hybridiuhkaan tähtäävästä toiminnasta ei voida hankkia tietoa tiedustelumenetelmien avulla. Näin ollen esimerkiksi hybridivaikuttamisessa hyödynnettävään informaatiovaikuttamiseen tai kybervaikuttamisen toimiin ei voida tiedustelumenetelmin puuttua, jos niitä toteutetaan kotirauhalla suojatusta asunnosta. Kun hybridivaikuttamisessa useimmiten hyödynnetään joko toista tai kumpaakin edellä mainituista vaikuttamiskeinoista, voidaankin pohtia, onko kotirauhan suojaaminen tiedusteluviranomaisen kansallisen turvallisuuden suojaamistehtävän ja näin ollen hybridiuhkien torjumisen kannalta hyvä vai huono asia.

Intressipunninnassa vastakkain ovat luonnollisen henkilön yksityisyyden suojan turvaaminen ja siihen puuttumiseen säädetty mahdollisimman korkea kynnys ja toisaalta valtion kansallisen turvallisuuden turvaaminen. Vastakkain ovat siis yksityisen etu ja yleinen etu. Kuten aiemmin tässä luvussa esitellyistä oikeustapauksista käy ilmi, on tärkeää, ettei yksityisyyden suojaan puututa viranomaisen toimesta tarpeettomasti tai mielivaltaisesti, joten kotirauhan suojaaminen sekä myös luottamuksellisen viestin salaisuuden suojaaminen on perusteltua. Tiedusteluviranomaisilla on kattavat toimivaltuudet jo nyt tiedon hankkimiseen, myös yksityisyyden suojalla turvatuista kohteista, jolloin yleinen etu menee yksityisen edelle. Siksi onkin mielenkiintoista, että juuri kotirauha on suojattu jopa luottamuksellista viestintää vahvemmin, ja ettei siihen ole kirjattu mahdollisuutta puuttua edes välttämättömästä syystä, kuten muihin yksityiselämän suojan osa-alueisiin.

4.2 Viranomaisten välinen tietojenvaihto ja viranomaisen työn tehokkuus

Tässä tutkielmassa on keskitytty viranomaisten tietojen antamiseen, joka tapahtuu viranomaisen toimesta joko oma-aloitteisesti tai laintasoisen säännöksen nojalla. Tutkielman keskiössä on ollut tiedustelutoiminnalla hankitun tiedon antaminen toiselle viranomaiselle ja samalla on ohuesti sivuttu myös henkilötietoja sisältävän tiedustelutiedon

luovuttamista. Tällä hetkellä erityisesti henkilötietojen vaihtaminen viranomaisten välillä on mahdollista vain erittäin perustellusta syystä ja lisäksi tietoa saa käyttää vain siihen käyttötarkoitukseen, johon se on kerätty[281]. Tietojen käyttötarkoitussidonnaisuus ilmenee vahvasti myös aiemmin luvussa 3.2.2 kuvatuista tiedustelulakien palomuurisäännöksistä, joiden mukaan tiedustelulla hankittua tietoa saa käyttää vain tiedustelutoiminnan käyttötarkoituksiin, eli kansallisen turvallisuuden suojaamiseksi tai sotilaallisen toiminnan selvittämiseksi. Laitinen ja Kuukasjärvi esittävät, että viranomaisten keskinäisellä tietojen vaihtamisella voidaan tehostaa viranomaisten työtä erityisesti ennalta estettäessä erilaisia uhkia, kuten hybridiuhkia, mutta se ei ole tällä hetkellä mahdollista kaikissa tarpeellisissa tilanteissa edellä kuvattujen perusteiden vuoksi. He näkevät suuren riskin siinä, jos tieto ei välity viranomaiselta toiselle tarkoituksenmukaisella tavalla, jolloin esimerkiksi hybridivaikuttamisen taustalla oleva toimija voi hyödyntää tiedonvaihdon jäykkyyttä osana vaikuttamistoimintaansa.[282]

Myös valtioneuvoston julkaiseman selvityksen mukaan viranomaisten välinen tietojen vaihtaminen on pitkälti reaktiivista, mikä ei aina mahdollista riittävästi viranomaisten ennakollista varautumista ja toimivaltuuksien käytön valmistelua kyberuhkatilanteisiin, eikä siten myöskään näiden uhkien ennalta-estämistä[283]. Sama pätee hybridiuhkia koskevaan tiedonvaihtoon, mikä osin johtuu hybridivaikuttamisen vaikeasti havainnoitavasta luonteesta, mutta myös tietojen luovutusta koskevan sääntelyn jäykkyydestä. On hyvä, että yksityistä henkilöä suojataan muun muassa kattavalla tietosuojalainsäädännöllä ja että viranomaisten toimintaa säännellään tarkasti yksityisen oikeusturvan turvaamiseksi, mutta Suomen maanpuolustuksen ja kansallisen turvallisuuden kannalta vihamielisen toiminnan tehokas estäminen edellyttäisi tiiviimpää yhteistyötä ja tiedonvaihtoa erityisesti uhkien havainnointivaiheessa, kuten valtioneuvoston selvityksestäkin käy ilmi[284]. Nykyisestä keskustelusta lainsäädännön kehittämiseksi on nähtävissä myön-

[281] HE 222/2022 vp, s. 6.
[282] Laitinen & Kuukasjärvi, 2023, s. 31.
[283] Valtioneuvosto, 2023a, s. 33.
[284] Valtioneuvosto, 2023a, s. 33.

teisempi suhtautuminen viranomaisten väliseen tietojen vaihtamiseen tai ainakin sellaisten tarpeettomien esteiden poistamiseen lainsäädännöstä tietojenvaihdon mahdollistamiseksi tilanteissa, joissa nykyinen lainsäädäntö estää tiedon antamisen toiselle viranomaiselle.

Yleisimmin esteet tietojen antamiselle johtuvat julkisuuslain salassapitoperusteista, joilla voidaan suojata yksityisen oikeusturvaa ja yksityiselämää sekä sellaisia viranomaisen hallussa olevia tietoja, jotka on katsottu julkisuuslain 24 §:n mukaisesti salassa pidettäviksi. Merkitystä salassapitoperusteiden soveltamisessa viranomaisten välisen tietojenvaihdon yhteydessä on salassapitoperusteen vahinkolausekkeilla ja niihin liittyvällä tilanne- ja tapauskohtaisella harkinnalla, joiden pohjalta arvioidaan, aiheuttaisiko tiedon antaminen vahinkoa salassapitoperusteessa säädetyllä tavalla[285]. Vahinkolausekkeet osoittavat, pohjautuuko salassapitoperuste julkisuusolettamaan vai salassapito-olettamaan, eli onko tieto lähtökohtaisesti julkinen vai salassa pidettävä ja millaista vaaraa tai vahinkoa tiedon antaminen voisi aiheuttaa[286]. Mäenpää on esittänyt esimerkkinä kohdan Eduskunnan oikeusasiamiehen 3.5.2005 antamasta ratkaisusta, jonka mukaan vahinkolausekkeiden tulkinta ei voi oikeuttaa viranomaista antamaan mitä tahansa tietoa toiselle viranomaiselle esimerkiksi hallinnon tehokkuuden nimissä, vaan tietojenanto-oikeudesta tulee olla laissa erilliset toimivaltasäännökset. Näin ollen mikään laissa viranomaiselle säädetty tehtävä ei yksinään luo toimivaltaa tietojen antamiselle, eikä se voi perustua myöskään viranomaisten toiminnan hyvään tarkoitukseen.[287]

Edellä mainitun pohjalta voidaan todeta, että tietojen vaihtaminen viranomaisten välillä ei olisi viranomaisten toiminnan tehokkuutta edistävä keino, tai ainakaan tehokkuus ei voisi olla ainoa peruste tietojen antamiselle, sillä toimivampi yhteistyö ja tiedon jakaminen kuitenkin edistäisivät viranomaisten toimintaa esimerkiksi kyber- ja hybridiuhkiin varautumisessa ja niitä ennakoitaessa. Myös OECD arvioidessaan Suomen julkishallinnon

[285] Mäenpää, 2023, s. 726.
[286] Mäenpää, 2023, s. 840.
[287] Mäenpää, 2023, s. 727. Mäenpää viittaa sivulla EOA:n 3.5.2005 antamaan ratkaisuun.

tilaa vuonna 2010 kiinnitti huomioita poikkihallinnollisen yhteistyön ja koordinaation kehittämiseen erityisesti sellaisissa monimutkaisissa politiikkahaasteissa, jotka vaativat nopeaa reagointia eivätkä sovittaudu selkeästi ainoastaan yhden organisaation toimialaan[288]. Hybridiuhat ovat nimenomaan esitetyn kaltaisia monimutkaisia haasteita, joihin vastaamiseen vaaditaan usein poliittista päätöksentekoa, kuten tänä talvena olemme saaneet huomata Suomen Itärajalla tapahtuvan välineellistetyn maahanmuuton kohdalla. Vaikka tässä tutkielmassa olenkin keskittynyt viranomaisten toimivaltuuksiin, tulee niiden käyttäminen kyseeseen hybridiuhkatilanteessa usein poliittisen päätöksen pohjalta, kun ylin valtiojohto on päättänyt ryhtyä toimenpiteisiin uhkan torjumiseksi.

[288] Valtiovarainministeriö, 2010, s. 18.

5 Johtopäätökset

Turvallisuusympäristömme on muuttunut radikaalisti erityisesti 2020-luvulla ja kansalliseen turvallisuuteemme vaikuttaa yhä enemmän kansainväliset tapahtumat ja uhkat. Suomen liityttyä puolustusliitto Natoon, kansallisen turvallisuutemme ja Euroopan unionin turvallisuuden lisäksi Suomen on omalta osaltaan turvattava myös Nato-maiden turvallisuutta. Moninaiset muutokset turvallisuusympäristössämme mahdollistavat myös uudenlaisten uhkien ja vaikuttamistoimijoiden ilmenemisen. Tutkielmassa käsiteltiin tällaisia uhkia ja vaikuttamistoimijoita hybridiuhkien, hybridivaikuttamisen ja hybridisodankäynnin näkökulmasta ja pohdittiin hybriditoiminnan ilmenemismuotoja ja tavoitteita. Vaikka useiden erilaisten keinojen hyödyntäminen esimerkiksi sodankäynnissä ei ole mitenkään uusi ilmiö, on digitalisaatio ja teknologinen kehitys mahdollistanut uudenlaisten ja huomaamattomampien keinojen hyödyntämisen osana vaikuttamistoimintaa. Tällaisia huomaamattomia ja monimutkaisia keinoja hybridivaikuttaja hyödyntää samanaikaisesti tai toistensa jatkumoina pyrkiessään vaikuttamaan toisen valtion perustavanlaatuisiin rakenteisiin ja horjuttamaan valtion päätöksentekoa ja sisäistä yhtenäisyyttä.

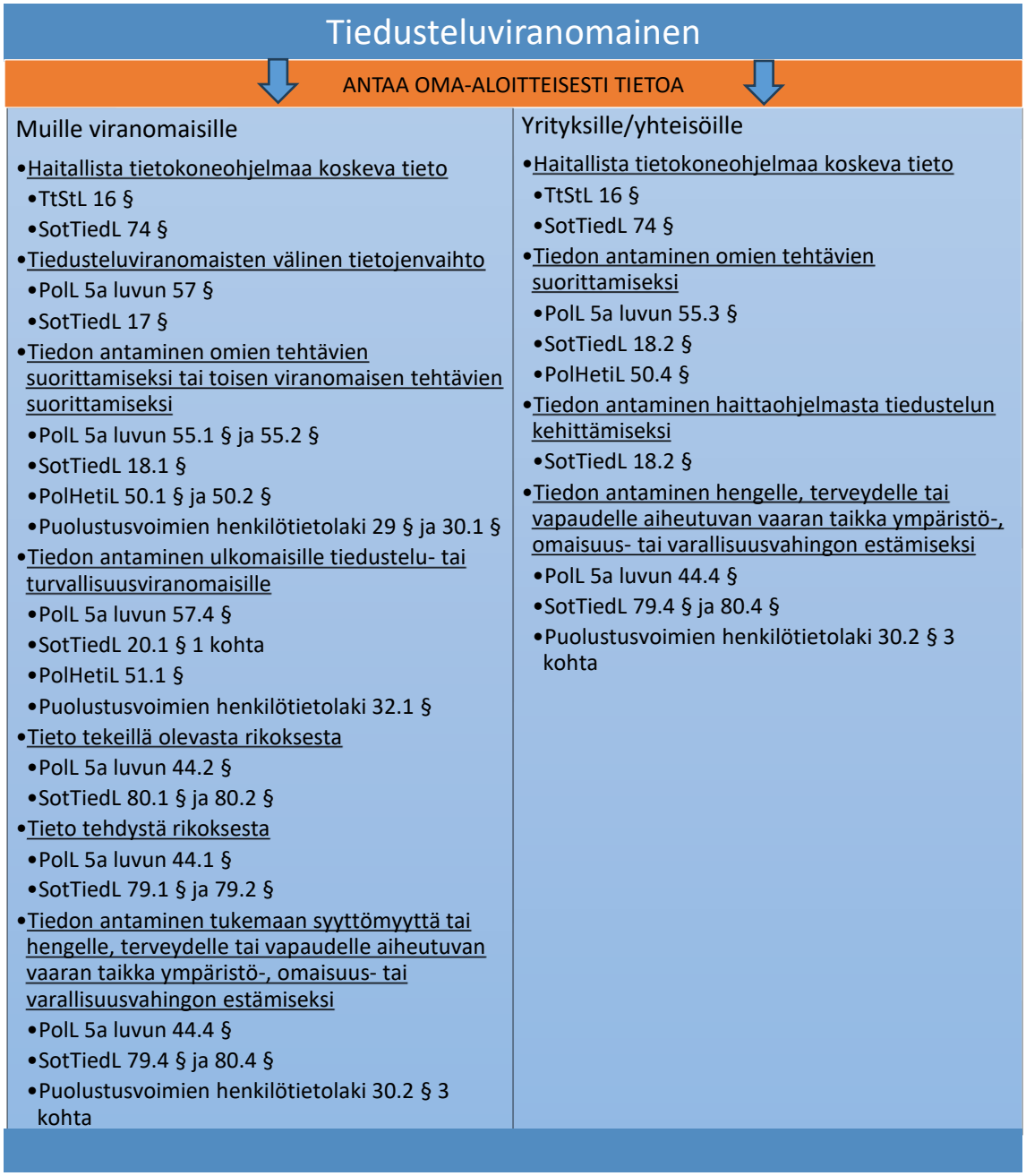
Muuttuneessa turvallisuusympäristössä lainsäädäntömmekin on kaivannut uudistamista, jotta uudenlaisia uhkia voidaan tunnistaa ja niihin kyetään vastaamaan viranomaisten toimivaltuuksin. Kansallista lainsäädäntöä on uudistettu kansallisen turvallisuuden parantamiseksi ja uudenlaisiin uhkiin vastaamiseksi muuttamalla muun muassa aluevalvontalakia (502/2017) vuonna 2017 sekä valmiuslakia (708/2022) ja rajavartiolakia (698/2022) vuonna 2022. Aluevalvontalain muuttamisella pyrittiin vastaamaan tunnuksettomien sotilaiden käyttämiseen Suomeen kohdistuvassa sotilaallisessa toiminnassa ja rajavartiolain muutoksella pyrittiin säätämään Rajavartiolaitokselle riittävät toimivaltuudet muuttoliikettä käyttävään hybridivaikuttamiseen vastaamiseksi. Samoin valmiuslain muutoksella luotiin toimivaltuudet poikkeusolojen käyttöönottoon erilaisissa hybridiuhkatilanteissa. Yksittäisten lakimuutosten lisäksi vuonna 2019 tuli voimaan siviili- ja sotilastiedustelua koskevat lait, joilla suojelupoliisille ja Puolustusvoimille tiedusteluviranomaisina annettiin toimivaltuudet tiedustelumenetelmien käyttämiseen kansallisen turvallisuuden ja sotilaallisen maanpuolustuksen turvaamiseksi.

Tutkielman aiheena oli tutkia tiedusteluviranomaisten toimivaltuuksia hybridiuhkien torjumiseksi sekä keskittyä erityisesti tiedusteluviranomaisten toimivaltuuksiin antaa tiedustelumenetelmin saatua hybridiuhkaan viittaavaa tietoa toiselle viranomaiselle tai muulle taholle oma-aloitteisesti. Tähän vastaamiseksi tutkimuksessa täytyi ensin perehtyä hybridiuhkiin ja miten niistä voidaan hankkia tietoa tiedustelumenetelmien avulla. Tutkimuksen ensimmäisenä tutkimuskysymyksenä oli; *Miten tiedusteluviranomaiset voivat torjua hybridiuhkia tiedustelulakien mukaisilla toimivaltuuksilla?* Kysymykseen vastaamiseksi toisen luvun tavoitteena oli alkuun määritellä oikeudellisesti mitä hybridiuhat ovat ja millaisin keinoin ja menetelmin niitä voidaan toteuttaa. Tämän jälkeen kuvattiin hybridiuhkien keinovalikoiman kannalta relevantit tiedusteluviranomaisten tiedustelutoimivaltuudet ja verrattiin näitä toimivaltuuksia hybridiuhkien havaitsemiseen ja torjumiseen.

Kolmannen luvun tavoitteena oli vastata tutkimuksen toiseen tutkimuskysymykseen, joka oli; *Miten hybridiuhkia voidaan torjua viranomaisten oma-aloitteisen tietojen antamisen avulla ja onko tiedusteluviranomaisilla riittävät toimivaltuudet oma-aloitteiseen tietojen antamiseen eri viranomaisille hybridiuhkien torjumiseksi?* Kysymykseen vastaamiseksi jäsenneltiin aluksi yleisesti viranomaisten tietojen antamista sääteleviä säännöksiä. Tämän jälkeen siirryttiin jäsentelemään nimenomaan tiedusteluviranomaisten tietojen antamista koskevia säännöksiä ja kuvaamaan niiden toimivaltuuksia tiedustelumenetelmin saadun, hybridiuhkaan viittaavan tiedon antamiseen. Tarkoituksena oli kuvata ne säännökset, jotka oikeuttavat tai velvoittavat tiedusteluviranomaisen antamaan hybridiuhkaan viittaavaa tiedustelutietoa toiselle viranomaiselle tai muulle taholle. Näin pystyttiin jäsentelemään ne säännökset, jotka mahdollistavat tiedusteluviranomaisten oma-aloitteisen tietojen antamisen toisille viranomaisille tai muille toimijoille, myös hybridiuhkatilanteessa. Lopuksi tutkielmassa kuvattiin lyhyesti vielä yksityisyyden suojan toteutumista tiedustelutoiminnassa ja yleisesti viranomaisten välistä tietojen vaihtamista viranomaistoiminnan tehokkuuden näkökulmasta.

Tutkimuksessa ilmeni, että tiedustelulakeja säädettäessä oli kattavasti huomioitu erilaiset uhkatekijät, joista voidaan hankkia melko laajasti tietoa tiedustelumenetelmin. Keskeisimmät hybridivaikuttamisen ja hybridisodankäynnin jo tunnistetut keinot oli tunnistettu tiedustelutoimivaltuuksia säädettäessä, minkä vuoksi niistä voidaan hankkia tietoa ennakollisesti uhkien tunnistamiseksi ja uhkien taustalla vaikuttavien tahojen selvittämiseksi. On kuitenkin huomioitava, että pahantahtoiset ulkopuoliset vaikuttajatoimijat pyrkivät hyödyntämään lainsäädännön mahdollisia aukkoja ja toimivaltuuksien epäselvyyttä, sekä kehittämään uusia keinoja näillä niin sanotuilla ”harmailla alueilla” toimimiseen. Näin ollen lainsäädännöllä ei pystytä täysin ennakoimaan erilaisia tulevaisuuden vaikuttamiskeinoja ja säätämään tyhjentävästi viranomaisten toimivaltuuksista kussakin yllättävässä ja uudenlaisessa tilanteessa. Tämä johtuu pitkälti siitä, että lailla ei voida säätää liian yleisiä toimivaltuuksia, joilla yleisesti voitaisiin ryhtyä ennalta määrittelemättömiin toimiin jonkin ennalta määrittelemättömän tapahtuman tai uhkan estämiseksi. Edellä mainittu liittyy ensi sijassa kansalaisten perusoikeuksien kunnioittamiseen ja turvaamiseen (PL 22 §) sekä siihen, että julkisen vallan käytön tulee perustua lakiin (PL 2.3 §). Näin ollen viranomaisten toimivaltuudet tulee säätää lailla eikä lailla säädetyillä toimivaltuuksillakaan voida antaa viranomaiselle rajatonta oikeutta puuttua perusoikeuksiin, vaan puuttumisen reunaehdot tulee kirjata lakiin.

Tiedustelutoimivaltuuksien avulla voidaan hankkia tietoa useista eri hybridiuhkan taustalla olevista vaikuttamiskeinoista, mutta miten kyseistä tietoa voidaan hyödyntää hybridiuhkien torjumiseksi. Tiedustelulla hankittu tieto on julkisuuslain 24.1 §:n 9–10 kohtien mukaan lähtökohtaisesti salassa pidettävää, mutta tiedustelulakien säännökset mahdollistavat tiedustelutietojen antamisen eteenpäin tietyissä tilanteissa. Myös tiedustelulla hankitut henkilötiedot ovat lähtökohtaisesti salassa pidettäviä. Seuraavassa kuviossa 4 on kuvattu tämän tutkimuksen myötä selvitetyt säännökset, jotka mahdollistavat tietyin edellytyksin tiedusteluviranomaisten oma-aloitteisen tietojen antamisen joko toisille viranomaisille tai yrityksille tai yhteisöille tiettyihin käyttötarkoituksiin. Kuvioon on listattu tietojen antamista koskevat säännökset ja eroteltu ne tiedon käyttötarkoituksen mukaan.



Kuvio 4. Tiedusteluviranomaisten oma-aloitteista tietojen antamista koskevat säännökset käyttötarkoituksittain.

Lähtökohtaisesti tiedusteluviranomainen voi kuviossa 4 mainituissa tilanteissa antaa tietoa kansallisen turvallisuuden tai maanpuolustuksen suojaamiseksi. Kuitenkin tieto tekeillä olevasta rikoksesta rikoksen torjumiseksi tai tehdystä rikoksesta rikoksen selvittä-

miseksi on mahdollista vain tietyistä tiedustelulakien palomuurisääntelyn sallimista rikoksista, jolloin muuta rikokseen liittyvää tietoa ei viimeisimmän Eduskunnan oikeusasiamiehen laintulkinnan mukaan voisi antaa kansallisen turvallisuuden tai maanpuolustuksen suojaamistarkoituksen nojalla. Palomuurisääntely on kirjattu poliisilain 5a luvun 44 §:n 1–2 momentteihin ja sotilastiedustelulain 79–80 §:ien 1–2 momentteihin.

Sen sijaan muista tiedustelulla hankituista tiedoista voi antaa tietoa toisille viranomaisille, jos se on tarpeen tiedustelutehtävien hoitamiseksi tai kansallisen turvallisuuden suojaamiseksi tai maanpuolustuksen kannalta (SotTiedL 18.1 § ja PolL 5a:55, 1–2). Samoin myös henkilötietoja voidaan antaa toisille viranomaisille, jos se on tarpeen tiedusteluviranomaisen tehtävien tai toisen viranomaisen tehtävien hoitamiseksi (PolHetiL 50 § 1–2 mom. ja Puolustusvoimien henkilötietolain 29 §). Kansainvälisessä yhteistyössä ulkomaan viranomaisille voidaan antaa tiedustelutietoja, jos se on tarpeen tiedusteluviranomaisen omien tehtävien tai kansallisen turvallisuuden suojaamiseksi (SotTiedL 20.1 § 1 kohta ja PolL 5a:57, 4) sekä henkilötietoja, jos se on välttämätöntä muun muassa kansallisen turvallisuuden suojaamiseksi (PolHetiL 51.1 § ja Puolustusvoimien henkilötietolain 32.1 §).

Lisäksi tiedot haitallisesta tietokoneohjelmasta voidaan antaa muille viranomaisille sekä yrityksille ja yhteisöille, jos se on tarpeen kansallisen turvallisuuden, maanpuolustuksen tai tiedon saajan etujen turvaamiseksi (SotTiedL 74 § ja TtStL 16 §). Tämän lisäksi sotilastiedusteluviranomainen saa antaa yrityksille tai yhteisöille haittaohjelman tunnistamistiedon tiedustelumenetelmien kehittämiseksi, jotta tiedustelutehtävä voidaan toteuttaa sekä muun kuin henkilötiedon, jos se on välttämätöntä Puolustusvoimien toiminnan tai kansallisen turvallisuuden suojaamiseksi (SotTiedL 18.2 §). Sen sijaan tiedustelutietoa voidaan aina antaa toisille viranomaisille syyttömyyden tueksi sekä hengelle, terveydelle tai vapaudelle aiheutuvan vaaran taikka ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi (SotTiedL 79.4 § ja 80.4 §, PolL 5a:44, 4). Lisäksi henkilötietoja voidaan antaa viranomaisille tai yrityksille ja yhteisöille, jos se on välttämätöntä edellä kuvattujen vaarojen tai vahinkojen estämiseksi (Puolustusvoimien henkilötietolain 30.2 §:n 3 kohta).

Kuten edellä kuvatusta käy ilmi, toimivaltuudet tiedusteluviranomaisten oma-aloitteiseen tietojen antamiseen löytyvät useista eri erityislaeista ja kyseiset säännökset säätelevät tiedon antamista hyvin tarkasti säännöksissä tarkoitetuissa tilanteissa. Niin tiedustelutietojen kuin tiedustelulla saatujen henkilötietojen antaminen on sidottu joko tietojen antamisen tarpeellisuuteen tai välttämättömyyteen, mikä kuvastaa korkeaa kynnystä näiden tietojen lähtökohtaiseen salassapitoon puuttumiseen.

Edellä kuvatut säännökset tietojen antamisesta voivat tulla kyseeseen myös hybridiuhkaan viittaavissa tilanteissa, jos kyseinen tieto viittaa hybridiuhkaan ja tiedon antamisen pohjalta toimivaltainen viranomainen tai esimerkiksi yritys voi ryhtyä toimiin uhkan torjumiseksi tai sen pysäyttämiseksi. Kun tiedusteluviranomainen saa tietoonsa haitallista tietokoneohjelmaa koskevan tiedon ja antaa sen oma-aloitteisesti toiselle viranomaiselle tai yritykselle tai yhteisölle, voidaan mahdollisesti torjua hybridivaikuttamisessa tai -sodankäynnissä hyödynnettävää kybervaikuttamista. Sama pätee tiedustelutiedon antamiseen toimivaltaiselle viranomaiselle sellaisesta toiminnasta, joka viittaa muunlaiseen hybridiuhkatoimintaan, jolloin toimivaltainen viranomainen voi ryhtyä toimiin uhkatoiminnan torjumiseksi tai pysäyttämiseksi.

Kansainvälisessä yhteistyössä hybridiuhkaan viittaavan tiedon antaminen voi mahdollisesti auttaa ulkomaisia tiedustelu- tai turvallisuusviranomaisia hankkimaan tietoa kyseisen toiminnan taustalla olevista tahoista ja aikeista, erityisesti jos hybridiuhkatoiminnan taustalla arvioidaan olevan rajat ylittävän järjestäytyneen rikollisryhmän tai muun ryhmittymän kaltaisia ei-valtiollisia toimijoita, mutta tietysti myös valtiollisia toimijoita. Kun tietoa annetaan kansainvälisessä yhteistyössä, muiden maiden tiedusteluviranomaiset voivat saada samaan asiakokonaisuuteen liittyviä tietoja omilla tiedustelumenetelmillään ja näin ollen antaa kyseistä tietoa myös Suomen tiedusteluviranomaisille, jolloin hybridiuhkaan viittaavasta toiminnasta pystytään luomaan parempaa kokonaiskuvaa Suomeen kohdistuvien toimien osalta.

Rikoksia koskevia tietoja sen sijaan ei voida kaikesta hybridiuhkaan viittavasta toiminnasta antaa toimivaltaisille rikostorjunta- ja esitutkintaviranomaisille, sillä tiedustelulakien palomuurisäännökset säätävät tietojen antamisesta vain sellaisista tehdyistä ja tekeillä olevista rikoksista, jotka täyttävät tietyn rikoslaissa säädetyn rangaistusasteikon. Lisäksi jo tehdyistä rikoksista ilmoittaminen ei auta hybridiuhkien torjunnassa, joten hybridiuhkien torjumisen näkökulmasta relevanteiksi tulee tekeillä olevista rikoksista tiedon antaminen.

Tekeillä olevien rikosten palomuurisääntely on kirjattu tiedustelulakeihin siten, että niistä on ilmoitettava, jos kyseisestä rikoksesta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta ja niistä saa ilmoittaa, jos kyseisestä rikoksesta säädetty ankarin rangaistus on vähintään 2 vuotta vankeutta. Tällaisia tiedusteluviranomaisen tietoon tulevia tekeillä olevia hybridiuhkaan viittaavia rikoksia voivat käsitykseni mukaan olla esimerkiksi erilaiset törkeät kyberrikokset, kuten törkeä tietoliikenteen häirintä (RL 38:6) ja törkeä tietojärjestelmän häirintä (RL 38:7 b), joista saa ilmoittaa rikostorjuntaviranomaiselle, sekä muun muassa tietyt terrorismirikokset ja useimmat rikoslain 12 ja 13 luvuissa säädetyt maanpetos- ja valtiopetosrikokset, joita voivat olla esimerkiksi luvaton tiedustelutoiminta (RL 12:9) ja laiton sotilaallinen toiminta (RL 13:4), joista on ilmoitettava rikostorjuntaviranomaiselle. Nämä esimerkit eivät ole tyhjentäviä, vaan ne osoittavat joitakin hybridiuhkan keinoja, joita koskevat tiedot voivat tulla tekeillä olevina rikoksina kyseisten säännösten mukaan sovellettavaksi.

Useimmiten hybridiuhkien synnyttämisessä kuitenkin pyritään hyödyntämään keinoja, joita ei luokitella rikoksiksi, joten lähtökohtaisesti muut tietojen antamista koskevat säännökset soveltuvat useimmiten tiedusteluviranomaisten oma-aloitteiseen tietojen antamiseen hybridiuhkien torjumiseksi. Näin ollen tietojen antaminen hybridiuhkien torjunnassa voisi useimmiten perustua palomuurisäännösten mukaiseen aina sallittuun tietojen antamiseen henkeä, terveyttä tai vapautta merkittävästi vaarantavan teon tai huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi, jolloin tiedon anta-

misella voitaisiin mahdollisesti torjua samalla hybridiuhkia. Kyseessä ei täydy olla rikokseen liittyvä tieto, vaikka säännökset ovatkin palomuurisäännöksissä, vaan tieto voisi nimenomaan liittyä kuvattujen vaarojen tai vahinkojen estämiseen.

Tutkimuksen pohjalta voidaan todeta ensimmäiseen tutkimuskysymykseen siitä*, miten tiedusteluviranomaiset voivat tiedustelutoimivaltuuksien avulla torjua hybridiuhkia*, että tiedusteluviranomaisilla on lähtökohtaisesti hyvät toimivaltuudet ryhtyä tiedonhankintaan toiminnasta, joka voi olla osa hybridivaikuttamista tai hybridisodankäyntiä. Ensi sijassa tietojen hankinta tiedustelumenetelmin auttaa hybridiuhkien torjunnassa ennakollisesti, jos tiedustelulla saadaan selville tietoa hybridiuhkaan tähtäävästä toiminnasta tai toiminnan suunnittelusta. Näin ollen tiedustelutoimivaltuudet auttavat nimenomaan hybridiuhkien ennakollisessa torjumisessa. Kun tiedusteluviranomainen saa tällaisesta toiminnasta tietoa ja epäilee toiminnan olevan luonteeltaan hybridiuhkaan tähtäävää toimintaa, voi se edellä kuvattujen säännösten ja niihin liittyvien hybridikeinojen tapauksissa antaa niitä koskevia tiedustelutietoja oma-aloitteisesti. Näin ollen toisen tutkimuskysymyksen ensimmäiseen osaan siitä, *miten hybridiuhkia voidaan torjua tiedusteluviranomaisten oma-aloitteisen tietojen antamisen avulla*, voidaan todeta, että tiedusteluviranomaisten tiedustelumenetelmin hankkimaa, hybridiuhkaan viittaavaa tietoa voidaan antaa oma-aloitteisesti laissa säädetyin edellytyksin kattavasti toisille viranomaisille ja muille tahoille. Oma-aloitteisen tietojen antamisen avulla uhkaavan toiminnan kohteet ja toimivaltaiset viranomaiset voivat ryhtyä hybridiuhkien torjumiseen paremmin, sillä ilman tiedusteluviranomaisilta saatua tietoa kyseisillä tahoilla tai viranomaisilla ei välttämättä olisi ollut riittävästi, tai ollenkaan, tietoa hybridiuhkaan tähtäävästä toiminnasta tai uhkan konkreettisuudesta.

Toisen tutkimuskysymyksen toiseen osaan siitä, *onko tiedusteluviranomaisilla riittävät toimivaltuudet oma-aloitteiseen tietojen antamiseen eri viranomaisille hybridiuhkien torjumiseksi*, voidaan todeta, että tiedusteluviranomaisilla on hyvin kattavat toimivaltuudet tiedon antamiseen toisille viranomaisille ja oma-aloitteista tietojen antamista koske-

vat säännökset kattavat useista hybridiuhkan osatekijöistä tiedon antamisen toisille viranomaisille tai tahoille. Näin ollen tiedustelun luonne, tiedustelutietojen lähtökohtainen salassapito ja yksityisyyden suoja huomioon ottaen tiedusteluviranomaiset voivat antaa hyvin tietoa oma-aloitteisesti hybridiuhkaan viittaavasta toiminnasta. Kuitenkin esimerkiksi uudet yhteistyöelimet, kuten Nato ja muut mahdolliset kansainväliset toimijat tulee ehkä huomioida kattavammin säädöksissä, sillä nykyiset kansainvälisen yhteistyön säännökset mahdollistavat tiedustelutietojen antamisen lähtökohtaisesti vain toisille ulkomaan tiedustelu- tai turvallisuuspalveluille. Lisäksi erilaisten toimijoiden rooli yrityskentällä tulisi tunnistaa paremmin tietojen antamista koskevissa säännöksissä.

Tietojen lähtökohtaisen salassapitovelvollisuuden vuoksi tietojen antaminen toisille viranomaisille on laajempaa kuin yrityksille, yhteisöille tai yksityisille henkilöille, sillä toisen viranomaisen samansisältöisestä salassapitovelvollisuudesta voidaan paremmin varmistua kuin yritysten, yhteisöjen ja yksityisten osalta. Salassapitosääntelyn käsittäessä tutkielman kannalta keskeisimmät tiedustelutiedot ja tiedustelumenetelmin hankitut henkilötiedot, on tiedusteluviranomaisen punnittava tarkasti tietojen antamisen merkitystä yleisen ja yksityisen edun sekä henkeen ja terveyteen kohdistuvien uhkien kannalta. Huomiota on erityisesti kiinnitettävä tiedustelulähteen turvaamiseen sekä yksityisyyden suojaamiseen, minkä vuoksi tietojen antaminen ei aina ole mahdollista, vaikka tiedon saajan olisikin tärkeää saada kyseinen tieto. Tiedustelulla puututaan usein yksityisyyden suojaan, minkä vuoksi puuttumisen keinot tulee olla säädetty lailla ja näillä keinoilla saatujen tietojen hyödyntämisen tulee olla lainmukaista, jotta yksityisyyden suoja ei tarpeettomasti kärsi. Näin ollen myöskään tiedusteluviranomaiset eivät voi kaikkea tiedustelutietoa jakaa toiselle toimivaltaiselle viranomaiselle, vaan annettavien tietojen tulee täyttää tarpeellisuuden vaatimukset, useimmiten joko tiedusteluviranomaisen tai toisen viranomaisen tehtävien hoitamiseksi.

Tutkimuksessa keskityttiin tiedusteluviranomaisten toimivaltuuksiin ryhtyä tiedonhankintaan kohteista, jotka voivat olla osa hybridivaikuttamista tai hybridisodankäyntiä ja

siten erilaisia hybridiuhkia. Lisäksi tutkimuksessa jäsenneltiin ne säännökset, joiden pohjalta tiedusteluviranomaiset voivat oma-aloitteisesti antaa hybridiuhkaan viittaavaa tiedustelutietoa muille tahoille tai viranomaisille. Hybridiuhkien torjunnassa myös muiden viranomaisten tietojen antamista koskevat säännökset ovat merkittävässä roolissa kattavan tiedonvaihdon turvaamiseksi. Siksi jatkotutkimuksessa voisi tutkia keskeisten turvallisuusviranomaisten toimivaltuuksia hybridiuhkien torjumiseksi, jotta voitaisiin selvittää, minkälainen merkitys tiedusteluviranomaisilta saaduilla tiedustelutiedoilla on uhkien torjuntaan ryhdyttäessä. Myös muiden viranomaisten toimivaltuuksia oma-aloitteiseen tietojen antamiseen hybridiuhkien torjumiseksi voisi olla hyvä selvittää tai esimerkiksi keskittyä pelkästään yhteen uhkatekijään, kuten kybervaikuttamiseen, ja selvittää viranomaisten toimivaltuuksia oma-aloitteiseen tietojen antamiseen kyberuhkien torjumiseksi.

Maailma muuttuu ja erilaisten uusien teknologioiden hyödyntäminen osana erilaisten toimijoiden vaikuttamistoimintaa ja jopa sotaa voi johtaa tuhoisiin seurauksiin. Teknologian ja digitalisaation mahdollistama kehitys on niin nopeaa, että lainsäädännöllä siihen ei välttämättä voida vastata riittävän ketterästi. Siksi hybridiuhkien torjumisessa keskeisessä roolissa on yhteiskunnan eri sektoreiden ja toimijoiden kriisinkestävyys yllättävissä muutoksissa, ja sama pätee myös yksilöihin. Ennakollinen tietojen antaminen havaituista toimista auttaa vähän, mutta tuntemattomasta toiminnasta tiedusteluviranomaiset eivät voi hankkia tietoa ennakollisesti. Kun toiminta yllättää, on tärkeää ryhtyä nopeasti toimiin uhkaavan toiminnan pysäyttämiseksi. Toiminnan pysäyttäminen on helpompaa sektorikohtaisten, mutta myös sektorirajat ylittävien, yhteisten tilannekuvien ja toimenpiteiden avulla, joita kokonaisturvallisuuden yhteistoimintamallilla edistetään ja ylläpidetään. Kun yhteiskunnan eri osa-alueet ovat yhdessä varautuneet erilaisiin uhkiin, on yllätyksellisistä tapahtumista helpompaa selvitä.

Lähteet

Aarnio, A. (1997). Oikeussäännösten systematisointi ja tulkinta: Ajatuksia teoreettisesta ja käytännöllisestä lainopista. Teoksessa J. Häyhä (toim.), *Minun metodini* (s. 35–56). Werner Söderström Lakitieto.

Aarnio, A. (2006). *Tulkinnan taito: ajatuksia oikeudesta, oikeustieteestä ja yhteiskunnasta.* Talentum Media Oy.

Aine, A., Nurmi, V-P. & Valtonen, V. (2022). Oikeuden resilienssi, perusoikeudet ja kokonaisturvallisuus. *Lakimies*, 6/2022, 841–872.

Bajarūnas, E. (2020). Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond. *European View*, 19(1), 62–70. https://doi.org/10.1177/1781685820912041

Björn, R. & Puistola, J-A. (2023). *Kansalaisen varautumisopas.* Docendo Oy.

Euroopan komissio. (2018). *Yhteinen tiedonanto Euroopan parlamentille, Eurooppa-neuvostolle ja neuvostolle: Selviytymiskyvyn ja valmiuksien kehittäminen hybridiuhkien varalta*. Noudettu 5.12.2023 osoitteesta https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:52018JC0016

Ferm, T. (2017). Laws in the era of hybrid threats. *Hybrid CoE*. Noudettu 1.11.2023 osoitteesta https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-3-laws-in-the-era-of-hybrid-threats/

Ferm, T. (2018). Ajankohtaista EU:n hybridiuhkien torjunnasta. *Defensor Legis,* 3/2018, 404–419.

Giannopoulos, G., Smith, H. & Theocharidou, M. (2021). *The landscape of Hybrid Threats: A conceptual model*. Publications Office of the European Union. https://dx.doi.org/10.2760/44985

Helsingin kaupunki. (2018). *Helsinki yhdistelmäuhkien aikakaudella – Yhdistelmävaikuttaminen ja kaupunki*. Helsingin kaupungin keskushallinnon julkaisuja 2018:22. Noudettu 30.10.2023 osoitteesta https://www.hel.fi/static/kanslia/Julkaisut/2018/hybridiraportti_fin_020818_netti.pdf

Heuru, K. (2003). *Hyvä hallinto*. Edita Publishing Oy.

Hirvonen, A. (2011). *Mitkä metodit?: opas oikeustieteen metodologiaan.* Yleisen oikeustieteen julkaisuja 17.

Hoffman, F. (2009). Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict. *Strategic Forum*, 240, 1–8. Noudettu 24.4.2024 osoitteesta https://www.files.ethz.ch/isn/98862/SF240.pdf

Huhtanen, R. (2010). Viranomaisten välinen tietojenvaihto ja yksityisen oikeusturva sosiaalioikeudessa. Teoksessa T. Tuominen (toim.), *Avoin, tehokas ja riippumaton: Olli Mäenpää 60 vuotta juhlakirja* (s. 55–68). Edita Publishing Oy.

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

Kaisto, J. (2005). *Lainoppi ja oikeusteoria: Oikeusteorian perusteista aineellisen varallisuusoikeuden näkökulmasta.* Edita Publishing Oy.

Kokonaisturvallisuuden sanasto. (2017). *Sanastokeskus TSK ry*. Noudettu 7.9.2023 osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Kokonaisturvallisuuden_sanasto.pdf

Kolehmainen, A. (2016). Tutkimusongelma ja metodi lainopillisessa työssä. Teoksessa T. Miettinen (toim.), *Oikeustieteellinen opinnäyte: Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta* (s. 106–131). Edita Publishing Oy.

Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. *Uusi tietosuojalainsäädäntö*. Alma Talent Oy.

Kulla, H. (2012) *Hallintomenettelyn perusteet*. Talentum Media Oy.

Kurvinen, E., Ahokas, K., Elmerot, Å., Hassinen, T., Havre, M., Kuukasjärvi, K., Laitinen, K., Launiala, M., Määttä, K., Salumaa-Lepik, K., Sariola, M., Tiura-Virta, H. & Voutilainen, T. (2023). *Oma-aloitteinen tietojen antaminen rikosten torjumiseksi*. Valtioneuvoston kanslia. http://urn.fi/URN:ISBN:978-952-383-216-9

Krakau, T. & Haapalehto, S. (2020). *Tietopyynnöt ja henkilötietojen luovuttaminen: opas julkisuuslain mukaisten tietopyyntöjen ja tietosuoja-asetuksen mukaisten henkilötietojen tarkastuspyyntöjen käsittelyyn sekä muihin tietojen luovutuksiin*. Alma Talent Oy.

Laitinen, K. & Kuukasjärvi, K. (2023). *Viranomaisten tietojenantaminen ja -vaihtaminen, tiedonkulku ja lainsäädäntö muuttuneessa turvallisuus- ja toimintaympäristössä*.

Poliisiammattikorkeakoulun katsauksia 34. Grano Oy. https://urn.fi/URN:NBN:fi-fe2023062157501

Lohse, M., Meriniemi, M. & Honkanen, K. (2019). *Tiedustelumenetelmät*. Alma Talent Oy.

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

Lonka, H., Laitinen, K., Keinänen, A., Wähä, S., Huhtinen, A. & Paasonen, J. (2020). *Kansallisen turvallisuuden vaikutusten arviointi*. Valtioneuvoston kanslia. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 2020:28. http://urn.fi/URN:ISBN:978-952-287-950-9

Mikkola, H., Aaltola, M., Wigell, M., Juntunen, T. & Vihma, A. (2018). *Hybridivaikuttaminen ja demokratian resilienssi: Ulkoisen häirinnän mahdollisuudet ja torjuntakyky liberaaleissa demokratioissa.* FIIA Ulkopoliittinen instituutti. Toukokuu 2018/55. Noudettu 24.4.2024 osoitteesta https://www.fiia.fi/wp-content/uploads/2018/05/fiia_report55_web_hybrdivaikuttaminen-ja-resilienssi.pdf

Mumford, A. & Carlucci, P. (2023). Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security, 8*(2), 192–206. https://doi.org/10.1017/eis.2022.19

Mäenpää, O. (2023). *Hallinto-oikeus*. Alma Talent Oy.

Mäenpää, O. (2020a). *Julkisuusperiaate*. Alma Talent Oy.

Mäenpää, O. (2020b). *Julkinen valta ja oikeusvaltio*. Helsingin yliopiston oikeustieteellinen tiedekunta.

Mäenpää, O. (2017). *Yleinen hallinto-oikeus.* Alma Talent Oy.

Mäenpää, O. (2002). *Hyvän hallinnon perusteet*. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja.

Määttä, K. & Hirvonen, M. (2018). *Viranomaisten tietojenvaihtosäännösten kehitys harmaan talouden ja talousrikollisuuden torjunnassa.* Edilex 2018/18. Edita Publishing Oy.

Määttä, T. & Paso, M. (2019). *Johdatus oikeudellisen ratkaisun teoriaan*. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja.

Määttä, T. (2016). Metodinen pluralismi oikeustieteessä – Ympäristöoikeudellisen tutkimuksen suuntaukset ja menetelmät. Teoksessa T. Miettinen (toim.), *Oikeustieteellinen opinnäyte: Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta* (s. 135–222). Edita Publishing Oy.

Neuvonen, R. (2017). *Oikeus julkiseen tietoon*. Helsingin Kamari Oy.

Neuvonen, R. (2014). *Yksityisyyden suoja Suomessa.* Lakimiesliiton kustannus.

Puolustusministeriö. (2015). *Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintalakityöryhmän mietintö*. Noudettu 5.12.2023 osoitteesta https://www.defmin.fi/files/3016/Suomalaisen_tiedustelulainsaadannon_suuntaviivoja.pdf

Räikkä, J. (2021). *Salaliittoteorioiden filosofia – Temppeliherroista liskoihmisiin*. Gaudeamus.

Saarikoski, E. (2022). *Tiedustelulait muuttuvassa hybridiuhkien maailmassa*. [pro gradu -tutkielma, Jyväskylän yliopisto]. JYX-julkaisuarkisto. http://urn.fi/URN:NBN:fi:jyu-202212195695

Sadik, G. (2017). *Europe's hybrid threats: What kinds of power does the EU need in the 21st century?.* Cambridge Scholars Publishing.

Sajama, S. (2016). Argumentaatio oikeustieteellisessä tutkimuksessa. Teoksessa T. Miettinen (toim.), *Oikeustieteellinen opinnäyte: Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta* (s. 24–50). Edita Publishing Oy.

Seppälä, P. (2011). Uhka käsitteenä. *Maanpuolustuskorkeakoulu, Strategian laitos.* Julkaisusarja 3, (N:o 16), Strategian asiatietoa. Noudettu 1.4.2024 osoitteesta https://www.doria.fi/bitstream/handle/10024/74127/StratL3_16w.pdf?sequence=1

Siltala, R. (2003). *Oikeustieteen tieteenteoria*. Suomalainen lakimiesyhdistys.

Sisäisen turvallisuuden sanasto. (2023). *Sanastokeskus TSK ry.* Noudettu 6.12.2023 osoitteesta https://intermin.fi/documents/1410869/4024872/Sisaisen_turvallisuuden_sanasto.pdf/

Sisäministeriö. (2018). *HE 202/2017 vp PuV 27.09.2018 lainsäädäntöneuvos Marko Meriniemi, sisäministeriö, asiantuntijalausunto*. Eduskunta. Noudettu 7.4.2024 osoitteesta https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-207774.pdf

Sisäministeriö. (2022). *Varautuminen muuttoliikettä hyväksikäyttävään hybridivaikuttamiseen – Selvitys lainsäädännön muutostarpeista*. Sisäministeriön julkaisuja 2022:20. https://urn.fi/URN:ISBN:978-952-324-577-8

Sisäministeriö. (2023a). *Kansallinen riskiarvio 2023*. Sisäministeriön julkaisuja 2023:4. https://urn.fi/URN:ISBN:978-952-324-602-7

Sisäministeriö. (2023b). *Asettamispäätös; Lainsäädäntöhanke siviilitiedustelulainsäädännön ja poliisin henkilötietolain 7 luvun tarkistamiseksi.* Noudettu 23.4.2024 osoitteesta https://api.hankeikkuna.fi/asiakirjat/9e6fe6e1-e4e6-4921-a17a-fd0b388a2928/92ebdeb3-bfbf-4397-882c-d522370bc6a4/ASETTAMISPAATOS_20231221095718.PDF

Smith, H. (2019). Countering hybrid threats. In G. Lindstrom & T. Tardy (Eds.), *NATO and the EU: The essential partners* (pp. 15–24). NATO Defense College. Noudettu 1.11.2023 osoitteesta http://www.jstor.org/stable/resrep19964.7

Tiedusteluvalvontavaltuutettu. (2020). *Tiedusteluvalvontavaltuutetun kertomus vuodelta 2019.* K 14/2020 vp. Noudettu 24.3.2024 osoitteesta https://tiedusteluvalvonta.fi/documents/12994206/22784442/Tiedusteluvalvontavaltuutetun+kertomus+vuodelta+2019/60544677-62f2-04f6-1c86-a54e7b66e102/Tiedusteluvalvontavaltuutetun+kertomus+vuodelta+2019.pdf

Turvallisuuskomitea. (2016). *Katsaus hybridiuhkiin ja niiden vaikutuksiin*. Noudettu 1.11.2023 osoitteesta https://turvallisuuskomitea.fi/katsaus-hybridiuhkiin-ja-niiden-vaikutuksiin/

Valtioneuvosto. (2020). *Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko*. Valtioneuvoston julkaisuja 2020:30. http://urn.fi/URN:ISBN:978-952-287-876-2

Valtioneuvosto. (2021a). *Valtioneuvoston puolustusselonteko*. Valtioneuvoston julkaisuja 2021:78. http://urn.fi/URN:ISBN:978-952-383-820-8

Valtioneuvosto. (2021b). *Valtioneuvoston selonteko tiedustelulainsäädännöstä.* Valtioneuvoston julkaisuja 2021:94. http://urn.fi/URN:ISBN:978-952-383-500-9

Valtioneuvosto. (2022). *Ajankohtaisselonteko turvallisuusympäristön muutoksesta*. VNS 1/2022. Valtioneuvoston julkaisuja 2022:18. http://urn.fi/URN:ISBN:978-952-383-772-0

Valtioneuvosto. (2023a). *Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa.* Valtioneuvoston julkaisuja 2023:31. https://urn.fi/URN:ISBN:978-952-383-542-9

Valtioneuvosto. (2023b). *Vahva ja välittävä Suomi - Pääministeri Petteri Orpon hallituksen ohjelma 20.6.2023*. Valtioneuvoston julkaisuja 2023:58. http://urn.fi/URN:ISBN:978-952-383-763-8

Valtioneuvoston kanslia. (2023). *Keskustelupaperi: Kognitiivinen intruusio - Miksi hybridivaikuttaminen toimii?* Valtioneuvoston kanslian julkaisuja 2023:14. https://urn.fi/URN:ISBN:978-952-383-440-8

Valtiovarainministeriö. (2010). *OECD:n Suomen hallinnon maa-arviointi - käännös tiivistelmästä ja keskeisistä suosituksista.* Noudettu 31.3.2024 osoitteesta https://vm.fi/documents/10623/307541/OECDn+arvioinnin+tiivistelm%C3%A4+ja+keskeiset+toimenpidesuositukset+suomeksi.pdf/ec2365e7-ef73-4154-b5dc-30c386198875/OECDn+arvioinnin+tiivistelm%C3%A4+ja+keskeiset+toimenpidesuositukset+suomeksi.pdf?t=1422530898000

Voimankäytön oikeussäännöt. (2015). Ulkoasianministeriö. Noudettu 5.12.2023 osoitteesta https://um.fi/documents/35732/48132/legal_grounds_for_the_use_of_force_in_international_relations

Voutilainen, T. (2021). KHO 2021:13 – Viranomaisen tiedonsaantioikeus. *Lakimies,* 3–4/2021, 676–687.

Yhteiskunnan turvallisuusstrategia. (2017). Valtioneuvoston periaatepäätös. *Turvallisuuskomitea*. Noudettu 8.9.2023 osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf

Virallislähteet

COM(2021) 891 final. Ehdotus Euroopan parlamentin ja neuvoston asetuksesta henkilöiden liikkumista rajojen yli koskevasta unionin säännöstöstä annetun asetuksen (EU) 2016/399 muuttamisesta.

EV 303/1998 vp. Eduskunnan vastaus hallituksen esitykseen laiksi viranomaisen toiminnan julkisuudesta ja siihen liittyviksi laeiksi.

HaVL 7/2018 vp. Hallintovaliokunnan lausunto perustuslakivaliokunnalle hallituksen esityksestä eduskunnalle laiksi Suomen perustuslain 10 §:n muuttamisesta.

HaVL 30/2021 vp. Hallintovaliokunnan lausunto puolustusvaliokunnalle valtioneuvoston puolustusselonteosta.

HaVL 19/2022 vp. Hallintovaliokunnan lausunto puolustusvaliokunnalle hallituksen esityksestä laeiksi valmiuslain ja asevelvollisuuslain 79 §:n muuttamisesta.

HaVM 31/1998 vp. Hallintovaliokunnan mietintö hallituksen esityksestä laiksi viranomaisen toiminnan julkisuudesta ja siihen liittyviksi laeiksi.

HaVM 10/2017 vp. Hallintovaliokunnan mietintö hallituksen esityksestä laiksi Euroopan hybridiuhkien torjunnan osaamiskeskuksesta.

HaVM 30/2018 vp. Hallintovaliokunnan mietintö hallituksen esityksestä siviilitiedustelua koskevaksi lainsäädännöksi.

HaVM 36/2018 vp. Hallintovaliokunnan mietintö hallituksen esityksestä siviilitiedustelua koskevaksi lainsäädännöksi.

HaVM 19/2021 vp. Hallintovaliokunnan mietintö valtioneuvoston selonteosta sisäisestä turvallisuudesta.

HaVM 35/2022 vp. Hallintovaliokunnan mietintö valtioneuvoston selonteosta tiedustelulainsäädännöstä.

HE 30/1998 vp. Hallituksen esitys eduskunnalle laiksi viranomaisten toiminnan julkisuudesta ja siihen liittyviksi laeiksi.

HE 198/2017 vp. Hallituksen esitys eduskunnalle laiksi Suomen perustuslain 10 §:n muuttamisesta.

HE 201/2017 vp. Hallituksen esitys eduskunnalle laeiksi rajavartiolain ja ulkomaalaislain muuttamisesta sekä eräiksi niihin liittyviksi laeiksi.

HE 202/2017 vp. Hallituksen esitys eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi.

HE 203/2017 vp. Hallituksen esitys eduskunnalle laiksi sotilastiedustelusta sekä eräiksi siihen liittyviksi laeiksi.

HE 258/2018 vp. Hallituksen esitys eduskunnalle kansallisen turvallisuuden huomioon ottamista alueiden käytössä ja kiinteistöomistuksissa koskevaksi lainsäädännöksi.

HE 63/2022 vp. Hallituksen esitys eduskunnalle valmiuslain ja asevelvollisuuslain 79 §:n muuttamisesta.

HE 94/2022 vp. Hallituksen esitys eduskunnalle laiksi rajavartiolain muuttamisesta.

HE 222/2022 vp. Hallituksen esitys eduskunnalle laeiksi eräiden kiinteistönhankintojen luvanvaraisuudesta annetun lain, valtion etuosto-oikeudesta eräillä alueilla annetun lain ja etuostolain 1 §:n muuttamisesta.

HE-luonnos 15.3.2024. Hallituksen esitys eduskunnalle laiksi väliaikaisista toimenpiteistä välineellistetyn maahantulontorjumiseksi. Noudettu 23.4.2024 https://api.hankeikkuna.fi/asiakirjat/c1846832-bfdc-4115-8b17-85dfaedf450a/d08119c3-40f4-44e3-86a7-1f7b19fc17cc/LAUSUNTOPYYNTO_20240315113602.PDF

LiVL 26/2018 vp. Liikenne- ja viestintävaliokunnan lausunto hallintovaliokunnalle hallituksen esityksestä eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi.

OMML 41/2016. Oikeusministeriön mietintö. Luottamuksellisen viestin salaisuus: Perustuslakisääntelyn tarkistaminen. http://urn.fi/URN:ISBN:978-952-259-533-1

PeVL 2/2008 vp. Perustuslakivaliokunnan lausunto maa- ja metsätalousvaliokunnalle hallituksen esityksestä laiksi maaseutuelinkeinohallinnon tietojärjestelmästä.

PeVL 18/2014 vp. Perustuslakivaliokunnan lausunto liikenne- ja viestintävaliokunnalle hallituksen esityksestä eduskunnalle tietoyhteiskuntakaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta.

PeVL 1/2015 vp. Perustuslakivaliokunnan lausunto sosiaali- ja terveysvaliokunnalle hallituksen esityksestä eduskunnalle laiksi työttömyysturvalain muuttamisesta.

PeVL 31/2017 vp. Perustuslakivaliokunnan lausunto sivistysvaliokunnalle hallituksen esityksestä eduskunnalle laiksi valtakunnallisista opinto- ja tutkintorekistereistä.

PeVL 62/2018 vp. Perustuslakivaliokunnan lausunto hallintovaliokunnalle hallituksen esityksestä laiksi henkilötietojen käsittelystä maahanmuuttohallinnossa ja eräiksi siihen liittyviksi laeiksi.

PeVL 21/2020 vp. Perustuslakivaliokunnan lausunto valtiovarainvaliokunnalle hallituksen esityksestä eduskunnalle valmisteverotusmenettelyn ja autoverotusmenettelyn uudistamista koskevaksi lainsäädännöksi.

PuVM 2/2022 vp. Puolustusvaliokunnan mietintö valmiuslain ja asevelvollisuuslain 79 §:n muuttamisesta.

UaVM 5/2022 vp. Ulkoasianvaliokunnan mietintö ajankohtaisselonteosta turvallisuusympäristön muutoksesta.

Ylimpien lainvalvojien ratkaisut

EOAK 23.11.2021. Dnro 289/2021. Tiedustelulainsäädännön ns. palomuurisääntelyn soveltaminen.

EOAK 29.1.2020. Dnro 811/2019. Asiakirjapyyntöön vastaaminen.

EOAK 23.11.2018. Dnro 4963/2017. Keskusrikospoliisille moitteet lausunnosta.

EOAK 29.11.2013. Dnro 1870/2013. Koiran avulla ei voi etsiä huumeita yleisellä paikalla.

EOAK 18.12.2003. Dnro 1634/4/01. Poliisin toimittama rippikoululeirin tarkastus.

OKA 20.9.2013. Dnro OKV/322/1/2012. Asiakirjapyynnön käsittely.

Kotimainen oikeuskäytäntö

KHO 2003:77

KHO 2007:39

KHO 2010:31

KHO 2012:8

KHO 2015:163

KHO 2017:82

KHO 2019:83

KHO 2020:4

Euroopan unionin tuomioistuimen ratkaisut

Yhdistetyt asiat C-293/12 ja C-594/12, Digital Rights Ireland ym., EU:C:2014:238

Euroopan ihmisoikeustuomioistuimen ratkaisut

EIT tapaus Klass ja muut v. Saksa, 6.9.1978

EIT tapaus Al-Nashif v. Bulgaria, 20.6.2002

EIT tapaus Weber ja Saravia v. Saksa, 29.6.2006

EIT tapaus Kennedy v. Yhdistynyt Kuningaskunta, 18.5.2010

EIT tapaus Zakharov v. Venäjä, 4.12.2015

EIT tapaus Szabó ja Vissy v. Unkari, 12.1.2016