LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Siviilitiedustelulainsäädännön vaikutukset yritysten liiketoiminnassa

Saalamo, Antti

2018 Laurea

Laurea-ammattikorkeakoulu

Siviilitiedustelulainsäädännön vaikutukset yritysten liiketoiminnassa

Antti Saalamo
Turvallisuusjohtaminen
Opinnäytetyö
Toukokuu, 2018

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusjohtaminen
Ylempi AMK

Antti Saalamo

Siviilitiedustelulainsäädännön vaikutukset yritysten liiketoiminnassa

Vuosi 2018 Sivumäärä 75

Yritysten omistaman tiedon suojaamisen tarpeet korostuvat digitalisoituvassa ympäristössä. Tämän opinnäytetyön tarkoituksena oli kuvata Suomessa käynnissä olevaa siviilitiedustelulainsäädännön kokonaishanketta sekä sen vaikutuksia yritysten liiketoimintaan. Tutkimuksessa keskityttiin erityisesti lakihankkeeseen sisältyvään tietoliikennetiedusteluun. Tästä aihekokonaisuudesta ei ole tehty paljoa tutkimusta. Työ pyrkiikin osaltaan selventämään, millaisia vaikutuksia käynnissä olevalla lainsäädäntöhankkeella voisi toteutuessaan olla suomalaiseen yhteiskunnalle ja elinkeinoelämälle.

Kyseinen tutkimus pohjautui laadulliseen tutkimukseen, jossa yhdistetään aihealueeseen liittyvää teoreettista tietoa ja empiiristä aineistoa. Käynnissä oleva tiedustelulainsäädäntöhanke on laaja kokonaisuus, joka koostuu sotilas- ja siviilitiedustelulain kokonaisuudesta. Opinnäytetyö käsitteli tiedustelulakihankekokonaisuutta siviilitiedustelun näkökulmasta huomioiden erityisesti erikseen syntyvän tietoliikennetiedustelulain mahdolliset vaikutukset suomalaiselle elinkeinoelämälle. Työn tutkimusaineistona on pääasiallisesti toteutetut asiantuntijahaastattelut sekä lainsäädäntöhankkeen kannalta eri työvaiheiden keskeisin kirjallinen materiaali.

Käynnissä oleva tiedustelulakihanke sai alkunsa vuonna 2013, jolloin Suomeen luotiin kyberturvallisuusstrategia. Siinä pohdittiin muun muassa lainsäädännön kehittämistä turvallisuusviranomaisten tiedonhankinnan ja tiedustelun näkökulmasta. Tiedustelulainsäädännön valmistelu jatkui vuonna kolmessa erillisessä työryhmässä vuonna 2015 siten, että sisäministeriö johti siviilitiedustelua koskevaa hanketta, puolustusministeriö sotilastiedustelua koskevaa hanketta ja oikeusministeriö perustuslain mahdollista muuttamista koskevaa hanketta. Sisäministeriön asettama siviililakityöryhmä luovutti mietintönsä alkuvuodesta 2017. Hallituksen esitys siviilitiedustelulainsäädännöstä luovutettiin eduskunnalle 25.1.2018.

Tiedustelulainsäädäntöhankkeella voidaan arvioida olevan monia tarpeita sekä hyötyjä niin kansallisen turvallisuuden kuin yleisestikin yhteiskunnan näkökulmista. Siviilitiedustelulainsäädännön valmistelussa on pyritty huomioimaan hankkeen mahdolliset vaikutukset myös kansantalouden, yritysten sekä elinkeinoelämän kannalta. Siviilitiedustelulain myötä suomalainen turvallisuusviranomaiskenttä muuttuisi siten, että suojelupoliisista tulisi siviilitiedusteluviranomainen, jonka toimivaltuudet perustuisivat poliisilain uudesta 5 a luvusta löytyviin tiedustelutoimivaltuuksiin. Tämän muutoksen myötä suojelupoliisi voisi muun muassa suorittaa tuomioistuimen luvalla tietyissä rajatuissa tilanteissa tietoliikennetiedustelua siihen tietoverkon osaan, joka ylittää Suomen rajan.

Haastatellut yhdeksän asiantuntijaa olivat kaikki sitä mieltä, että Suomeen tarvitaan selkeä ja tarkoin säädelty tiedustelulainsäädäntö. Tutkimuksen johtopäätöksenä esitetään, että käynnissä oleva hanke on suomalaisen yhteiskunnan turvallisuuden kannalta merkittävä. Yritysten tulisi perehtyä sen tuomiin vaikutuksiin oman liiketoimintansanäkökulmasta. Opinnäytetyöhön on koottu selkeä ohjeistus, jonka avulla yritykset voivat arvioida tulevan lainsäädännön vaikutuksia omaan liiketoimintaan ja valmistautua muutoksiin.

Asiasanat: tiedustelulainsäädäntö, siviilitiedustelu, tietoliikennetiedustelu, kyberturvallisuus

Laurea University of Applied Sciences **Abstract**
Degree Programme in Security Management
Master's Thesis

Antti Saalamo

The impacts of the civilian intelligence legislation in the business acivities of companies

Year 2018 Pages 75

Companies have a great need to protect their intellectual property in the present digitalized environment. The purpose of this Master's thesis is to describe the ongoing process regarding the proposal for legislation on civilian intelligence in Finland and its effects on companies' business activities. The study focuses especially on network traffic intelligence which would be a part of the civilian intelligence integrity. At the moment there is little research done from this in area and this study aims to clarify what the possible impacts for the Finnish society and for the economic life would be if these intelligence laws would come into effect.

This Master's thesis is based on qualitative study which combines theoretical data and empirical material. The ongoing process regarding creating intelligence laws in Finland is a broad whole which consists of Military Intelligence Act and Civilian Intelligence Act. The study addresses the intelligence entity from the civilian intelligence perspective taking the arising Network Traffic Intelligence Act especially into account. Mainly the theoretical basis consists of professional interviews and the fundamental written material of the legislation process.

The current legislation process started in 2013 when the cyber security strategy was established in Finland. This strategy considered the need for developing the legislation regarding intelligence gathering methods and intelligence in general by the Finnish authorities. The preparation of the intelligence legislation continued in 2015 so that the Ministry of the Interior was responsible for the civilian intelligence legislation, the Ministry of Defence was responsible for the military intelligence legislation and the Ministry of Justice was responsible for the possible alteration of the Finnish constitution. The working group for the Ministry of Interior handed over its report in early 2017. The government proposal for the Civilian Intelligence Act was released on the 25th of January 2018 for the Parliament of Finland.

The intelligence legislation has many requirements and benefits from the national security point of view and in general for the Finnish society. The working group responsible for the Civilian Intelligence Act aimed to take into account the possible impacts for public economy and for the private sector. The Civilian Intelligence Act would alter the field for security authorities in a way that the Finnish Security Intelligence Service would start to operate as a civilian intelligence authority. Chapter 5 a in the Police Act would contain the intelligence gathering methods that the civilian intelligence authority would have in its jurisdiction. Due to this change The Finnish Security Intelligence Service would have the power in certain cases to technically gather network traffic intelligence in the communications network that crosses the Finnish border.

All of the nine interviewed specialists agreed that there is a need for a clear and accurately regulated intelligence legislation in Finland. The conclusion of the Master's thesis was that the ongoing intelligence legislation process is significant for the Finnish society and companies should familiarize themselves with the upcoming changes from the perspective of their business.

Keywords: intelligence, civilian intelligence legislation, network traffic intelligence, cyber security

Sisällys

1 Johdanto

Ihminen on kautta aikojen ollut kiinnostunut tiedosta. Tieto ja ymmärrys on ollut aikoinaan jo Antiikin Rooman valtakunnan menestyksen perustana, kun keisarin joukot suorittivat tiedustelutoimintaa vihollisen liikkeistä ja pystyivät näin ohjaamaan omia vastatoimia tehokkaasti. Toisen maailmansodan aikana tiedustelutoiminnalla oli merkittävä rooli ja muun muassa saksalaisten Enigma-salauslaitteen käyttämän salauksen purkamisen arvioidaan lyhentäneen sodan kestoa noin kahdella vuodella (BBC 2012).

Euroopassa useimmilla mailla on omat tiedustelupalvelunsa sekä tiedustelutoimintaa säätelevät lakinsa. Suomi on ollut tässä suhteessa hyvin poikkeava, sillä Suomella ei ole minkäänlaista lainsäädäntöä tiedustelutoiminnan kannalta. Olemme olleet tässä asiassa monia Euroopan maita jäljessä peräti muutamia vuosikymmeniä ja osin tästä syystä Suomi on kohdannut muutamia vakavia turvallisuustapahtumia.

Suojelupoliisin mukaan ulkoministeriö on joutunut kaksi kertaa vakavan verkkovakoilun kohteeksi. Vuonna 2013 paljastuneiden vakoilutapausten taustalla on suojelupoliisin mukaan valtiollinen taho, mutta tarkempaa tietoa toimintaa suorittaneesta maasta ei ole. Vakavampaa vakoilutapausta suojelupoliisi kuvailee erittäin edistykselliseksi ja vaikeasti havaittavaksi. Ulkoministeriöstä vietiin tapausten johdosta runsaasti materiaalia, mutta viranomaiset eivät ole julkaisseet tarkempia tietoja vuodetusta aineistosta. (Yleisradio 2014.)

Vuonna 2013 julkistettiin Suomen kyberturvallisuusstrategia, jonka pohjalta valtionjohto käsitteli myös tiedustelulainsäädännön tarpeellisuutta. Osana tämän strategian toimeenpanoaasetettiin erillinen tiedonhankintalakityöryhmä selvittämään tiedustelua koskevan lainsäädännön kehittämistarpeita. Työryhmän tammikuussa 2015 julkaisemassa mietinnössä ehdotettiin, että hallitus käynnistäisi erilaiset toimet tiedustelua koskevan lainsäädäntöperustan luomiseksi. (Eduskunta 2018.)

Suomen kaltaisen yhteiskunnan digitalisaatiokehitys kiihtyy. Tämä tarkoittaa myös sitä, että yhteiskuntaan kohdistuvien uhkien toimintaympäristössä on tapahtunut suuria muutoksia. Vakavimmat kansallisen turvallisuuden uhat tulevat nykyisellään miltei poikkeuksetta ulkomailta. Nämä uhkat ovat myös siirtyneet entistä enemmän tietoverkkoihin. Tästä syystä Suomessakin tiedonhankintaa tulisi ulottaa myös tietoverkkoihin. Tiedustelumenetelmät ovat myös kehittyneet ja luotettavan sekä ajantasaisen tiedon merkitys on kasvanut. (Karjalainen 2017.)

Puolustusministeriön vuonna 2013 asettaman tiedonhankintalakityöryhmän mietinnön mukaan tietoverkoissa tapahtuvan kybervakoilun ja -operaatioiden merkitys tulee kasvamaan entisestään tulevien vuosien aikana. Mahdollisia syitä tälle kehitykselle voivat olla muun muassa ope-

raatioiden toteuttaminen kyberympäristöissä alhaisilla kustannuksilla, kohteen suojaamisen vaikeus sekä kalleus sekä melko vähäinen kiinnijäämisriski. Kaikki Suomen turvallisuuspoliittisen kehityksen näkökulmasta olennaiset ulkovallat kehittävät sekä panostavat päämäärätietoisesti hyökkäyksellisen kyberkyvykkyyksiensä rakentamiseen. Työryhmän mietintö arvioi, että terroristisessa tarkoituksessa suoritettujen kyberhyökkäysten uhka Suomea kohtaan on melko rajallinen, mutta toisaalta tilanne voi muuttua nopeasti kansainvälisessä toimintaympäristössä tapahtuvien kehitysten seurauksena. (HE 202/2017 vp.)

Nykyisellään lainsäädännön sisältämät erilaiset tiedonhankintakeinot ovat puhtaasti rikostorjunnan tarpeisiin, mikä ei ole tiedustelutoimintaa, eikä niitä toimivaltuuksia voida käyttää muuhun kuin rikostiedusteluun. Nykyisellään toimivaltuudet on sidottu vahvasti rikoksen käsitteeseen, kun taas tiedustelutoiminnalla pyritään saamaan tietoja muun muassa kansallista turvallisuutta vakavasti uhkaavasta toiminnasta ja sen riittävän varhaisessa vaiheessa tapahtuvasta havaitsemisesta. Tällä hetkellä kansallisen turvallisuuden uhkat ovat luonteeltaan usein sellaisia, että niitä ei Suomen lain mukaan pidetä rikoksina. Pelkästään edellä mainituista syistä tarvitaan uutta lainsäädäntöä. (Meriniemi 2017.)

Käytännössä tiedustelulainsäädäntöhanke käynnistyi lokakuussa 2015, minkä pohjalta muun muassa sisä-, puolustus- ja oikeusministeriö käynnisti omat selvityksensä erityisesti hankkeen lainsäädännöllisistä vaatimuksista sekä muutoksista. Sisäministeriö asetti syksyllä 2015 monialaisen työryhmän, jonka tehtävänä oli muodostaa ehdotus siviilitiedustelua koskevaksi lainsäädännöksi. Samaan aikaan puolustusministeriö asetti oman työryhmänsä valmistelemaan sotilastiedustelua koskevaa lainsäädäntöä. Oikeusministeriön tehtävänä oli selvittää tiettyjen edellytysten täyttyessä kansallisen turvallisuuden suojaamiseksi tarpeellisten rajoitusten käyttöönotosta liittyen luottamuksellisen viestin suojaan, mikä on vahvasti suojattu perustuslain näkökulmasta.

Tiedustelulakikokonaisuutta valmistelleet työryhmät luovuttivat mietintönsä alkuvuodesta 2017, jonka jälkeen mietinnöt olivat lausuntokierroksella. Tammikuussa 2018 sisäministeri Paula Risikko esitteli siviilitiedustelulainsäädäntöä koskevan hallituksen esityksen eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi (HE 202/2017 vp). Kyseisen esityksessä ehdotetaan, että uusi siviilitiedustelua koskeva luku lisättäisiin poliisilakiin sekä säädettäisiin kokonaan uusi laki tietoliikennetiedustelusta siviilitiedustelussa. Suojelupoliisille esitetään erillisiä tiedustelutoimivaltuuksia, jotka olisivat voimassa sekä Suomessa, että ulkomailla. Tiedustelutoimivaltuudet saisivat pohjansa menetelmällisesti rikostorjunnassa käytettävistä toimivaltuuksista. (Sisäministeriö 2017.)

Viimeaikaiset tapahtumat Suomessa, joihin voidaan lukea Turussa elokuussa 2017 tapahtunut puukkoisku, ovat vauhdittaneet tiedustelulainsäädännön voimaantuloa jo tällä vaalikaudella

(2015-2019). Tämä puolestaan vaatisi lainsäädäntökokonaisuuden säätämistä kiireellisenä sekä 5/6:n enemmistöä eduskunnassa, koska kokonaisuus vaatii muutoksia myös perustuslakiin.

Tiedustelulainsäädännöllä ja erityisesti siviilitiedustelulainsäädännöllä tulee olemaan vaikutuksia myös elinkeinoelämään ja yritysten toimintaan. Aiheesta ei ole tehty juurikaan tutkimusta Suomessa, todennäköisesti siitä syystä, että lainsäädäntö on vielä valmisteluvaiheessa. Osittain näistä syistä tämä tutkimus on saanut alkunsa.

2 Opinnäytetyön lähtökohdat

Mielenkiintoni käynnissä olevaa tiedustelulakihanketta kohtaan alkoi lakeja valmistelevien työryhmien töiden aikana. Vuonna 2015 alkanut eri ministeriöiden työryhmien työskentely huomioitiin julkisessa keskustelussa varsin laajasti. Keskustelu keskittyi kuitenkin melko vahvasti osittain vinoutuneesti vain tiettyihin osa-alueisiin. Ensinnäkin Suomi on tunnettu vahvasta yksityisyydensuojasta ja tiedustelulakien valmistelu nähtiin melko vahvasti hyökkäyksenä tuon suojan murentamiseen, jopa massavalvonnasta puhuttiin. Toiseksi huomio oli kiinnittynyt pitkälti kansallisen turvallisuuden sekä ajantasaisen uhka- sekä havaintotiedon parantamiseen. Yleisesti esimerkiksi kansallinen turvallisuus, jota ei ole edelleenkään määritelty lainsäädännössä tarkasti, nähtiin esimerkiksi terrorismintorjunnan tai valtiollisen vakoilutoiminnan estämisen näkökulmasta. Itseäni ihmetytti keskustelun näkökulmien puute, koska Suomen kansalliseen turvallisuuteen kuuluu olennaisesti myös esimerkiksi kansallisten taloudellisten intressien suojaaminen. Tämän vuoksi kyseistä tiedustelulakihanketta tulisi tarkastella myös yritysmaailman näkökulmasta ja tarvittaessa lisätä tietoisuutta siitä, millaisia vaikutuksia tai minkälaisia toimenpiteitä suomalaisten yritysten tulisi tehdä, jotta ne voisivat huomioida käynnissä olevan lainsäädäntöhankkeen toiminnassaan myös tulevaisuudessa.

Käynnissä oleva lakihanke pitää sisällään tai ainakin sivuaa läheisesti merkittäviä osa-alueita yritysten toiminnan näkökulmasta. Ensinnäkin lakikokonaisuuksien valmisteluissa määritelty tietoliikennetiedustelu sekä ulkomaan tietojärjestelmätiedustelu liittyvät olennaisena osana kyberturvallisuuteen sekä yritysten kokonaisturvallisuusajatteluun. Kyberturvallisuus näyttelee tällä hetkellä merkittävää roolia yritysten tietopääoman sekä yleisen toiminnan jatkuvuuden suojaamisen kannalta. Siksi onkin tärkeätä huomioida myös kyberturvallisuuden rooli ja taso nykyisellään suomalaisessa elinkeinoelämässä, jotta tiedustelulakikokonaisuutta tarkastella laajemmin yritysten näkökulmasta.

Toiseksi yritysten toimintaan tulee vaikuttamaan Euroopan Unionin tietosuoja-asetus GDPR (General Data Protection Regulation), jota yritysten tulee noudattaa 25.5.2018 alkaen. Tietosuoja-asetusta sovelletaan lähtökohtaisesti kaikessa henkilötietoihin liittyvässä käsittelyssä. Henkilötietoja ylläpitävän rekisterinpitäjän tulee huolehtia siitä, että GDPR-asetuksessa määriteltyjä tietosuojaperiaatteita noudatetaan kaikissa tiedon käsittelyvaiheissa. Uuden lainsää-

dännön tarkoituksena on parantaa muun muassa henkilötietojen suojaa ja rekisteröityjen oikeuksia, yhteinäistää tietosuojan sääntelyä kaikissa EU-maissa sekä vastata uusiin digitalisaation ja globalisaatioon kuuluviin tietosuojakysymyksiin. (Tietosuojavaltuutetun toimisto 2018.)

Kyseinen tietosuoja-asetus liittyy osaltaan myös tiedustelulainsäädännön tuomiin haasteisiin, koska asetus patistaa rekisterinpitäjiä ja yrityksiä tekemään määräaikaan mennessä muun muassa henkilötietojen käsittelystä arvion sen nykytilasta ja analyysin siitä, että vastaavatko yrityksen henkitietojen sekä tietosuojan käsittelyä koskevat käytänteet kansallisen lainsäädännön ja EU:n tietosuoja-asetuksen uusia vaatimuksia. Lähtökohtaisesti kyseinen asetus lähtee siitä, että yritysten ja organisaatioiden tulee varmistaa tietoturvansa tarpeellinen riittävyys sekä luoda varautumissuunnitelmat erilaisten ongelmatilanteiden varalta. Tiedustelulainsäädännön näkökulmasta yritysten tulisi myös varmistua siitä, että heidän tietopääomansa sekä tietosuojakäytänteensä ovat riittävät mahdollisten tiedustelulainsäädännön myötä tulevien muutosten suhteen. (Tietoviikko 2018.)

Yritysten tarpeet suojata tietoa nykyisessä digitalisoituvassa ympäristössä korostuvat ja suoranaisen luottamuksellisen tiedon merkitys korostuu. Yrityssalaisuudella tarkoitetaan yritystoiminnan kannalta merkityksellistä sekä omistajalleen kilpailuetua antavaa tietoa, jonka taloudellinen arvo perustuu sen sisällön ja varsin usein myös sen olemassaolon salassa pitämiseen. Hyvin usein yrityssalaisuudet ilmenevät muun muassa paperisina asiakirjoina tai nykyisellään tietojärjestelmissä säilytettävään dataan ja tuoteprototyyppeihin. Yrityssalaisuuden luonne on usein aineetonta, joten sitä ei voi sellaisenaan anastaa, luovuttaa tai kätkeä. (Oittinen 2017, 1.)

Yksityisen ja julkisen sektorin toiminta on digitalisoitumiskehityksen myötä siirtynyt entistä enemmän kybertoimintaympäristöön, jossa myös toimintaa uhkaavat riskit ovat moninaiset. Kyberuhalla tarkoitetaan mahdollisuutta sellaiseen kybertoimintaympäristössä vaikuttavaan tekoon tai tapahtumaan, joka toteutuessaan voi vaarantaa jonkin toiminnon, joka on riippuvainen kybertoimintaympäristöstä (Oittinen 2017, 5). Osin näistä lähtökohdista Suomessakin käynnissä oleva tiedustelulainsäädäntöhanke on käynnistynyt. Lainsäädännöllä pyritään luomaan viranomaisille toimivaltuudet, joilla pystyttäisiin havaitsemaan ja torjumaan myös kybertoimintaympäristöissä tapahtuvia uhkia.

2.1 Aiheen avaaminen ja työn tavoite

Nykyinen yhteiskuntamme nauttii digitalisoitumisen myötä tulleista mahdollisuuksista ja samalla luotamme siihen, että biteistä muodostuva sähköinen maailma on turvallinen. Kybermaailmasta ja kyberturvallisuudesta on tullut erottamaton osa arkeamme. Globaali talous,

yhteiskuntien turvallisuus, yritysten toiminta ja elämäntapamme ovat tänä päivänä hyvin riippuvaisia tietojärjestelmien ja -verkkojen toimivuudesta. Megatrendinä on nähtävissä, että riippuvuutemme bittien turvallisesta toiminnasta lisääntyy kiihtyvällä vauhdilla. (Limnéll et al. 2014, 13.)

Vaikka digitalisoituminen on kehittänyt julkista ja yksityistä sektoria merkittävästi, on se tuonut mukanaan myös uudentyyppisiä uhkia erityisesti yhteiskunnan toiminnan kannalta. Kyberturvallisuuden merkitys erityisesti yhteiskunnan kriittisten toimintojen kannalta on nykypäivänä merkittävä. Valtiollisessa mielessä kybertoimintaympäristö on muuttunut myös osaksi sotilaallista toimintaa. Heikki Tiilikaisen Hybridisota-kirjan mukaan kybersodalla tarkoitetaan murtautumista poliittisista syistä vihollisen tietojärjestelmiin tekemään sabotaaseja ja suorittamaan vakoilua. Kybersota on siis yksi osa laajempaa informaatiosodankäyntiä ja siihen liittyvä toiminta, vaikka digitaalisesti tapahtuukin, voi aiheuttaa suunnattomia tappioita yhteiskunnalle ja sen väestölle. Siksi monet asiantuntijat pitävätkin kybersotaa perinteisen sodankäynnin uutena muotona. Esimerkiksi Yhdysvallat on julkaissut uuden kyberstrategiansa, jonka puitteissa lisätään asevoimien kykyä vastata maahan kohdistuneisiin hyökkäyksiin ”kyberaseilla”. (Tiilikainen 2015, 77.)

Suomessa vuonna 2013 perustettu tiedonhankintaa sekä tiedustelulainsäädännön tarvetta pohtinut työryhmä toi mietinnössään (Puolustusministeriö 2015b) esiin sen, että maahan tarvitaan tiedusteluun oma lainsäädäntönsä, jotta pystytään havaitsemaan ja ehkäisemään erityisesti tietoverkoissa vakavasti kansallista turvallisuutta uhkaavia tapahtumia sekä ilmiöitä.

Elinkeinoelämällä ja yrityksillä on suuri merkitys kansantalouden kannalta, mitä pyritään myös suojaamaan valmistellulla tiedustelulainsäädännöllä. Elinkeinoelämän tutkimuslaitoksen tekemän tutkimuksen (Etla 2016, 4) mukaan vuonna 2015 Suomen kymmenen tärkeintä yritystä tuottivat yhteensä 7,5 prosenttia Suomen kokonaisbruttokansantuotteesta. Tämä luku pitää sisällään ainoastaan yritysten itse tuottaman arvonlisän, mutta eivät erilaisia kerrannaisvaikutuksia. Vertailun vuoksi Suomessa toimivien pienten- ja keskisuurten yritysten osuus bruttokansantuotteesta vuonna 2016 oli runsaat 40 prosenttia (Suomen yrittäjät 2018).

Yllä mainituista syistä lähdin hahmottelemaan opinnäytetyön tavoitteita. Käynnissä olevaa tiedustelulainsäädäntöhanketta on käyty läpi julkisuudessa enemmän yksityisyydensuojan ja massavalvonnan näkökulmista ja elinkeinoelämän ja lainsäädännön vaikutusten arviointi yritysten kannalta on puuttunut miltei kokonaan. Nykyisellään ulkovaltojen sekä järjestäytyneen rikollisuuden yritysvakoilu aiheuttaa merkittäviä uhkia erityisesti suomalaisille korkean teknologian yrityksille. Niiden ydinliiketoiminta perustuu aineettomaan tietopääomaan, jonka paljastuminen aiheuttaisi muun muassa taloudellista haittaa kohdeyritykselle.

Tämän tutkimuksen tavoitteena on tuottaa uutta tietoa eritoten käynnissä olevan siviilitiedustelulainsäädännön sekä uuden tietoliikennetiedustelun mahdollisista vaikutuksista yritysten toiminnassa. Työn alaluku 7.3 sisältää yrityksiä varten tehdyn koosteen valmistellusta tietoliikennetiedustelusta. Tiedustelulainsäädännön jatkotutkimustarpeita käsitellään alaluvussa 7.4, mistä löytyy myös yrityksille ja lainsäätäjälle kehitysehdotuksia siviilitiedustelun onnistuneen käytännön toteuttamisen näkökulmasta. Tutkimusta varten tehtyjen haastatteluiden perusteella oli havaittavissa, että yrityksillä ei ole tällä hetkellä tarkkaa kuvaa siitä, että millaisia muutoksia tai velvoitteita tiedustelulainsäädäntö toteutuessaan toisi yritysten toimintaan ja tätä kautta koko suomalaiseen yhteiskuntaan.

2.2 Tutkimuskysymyksen asettaminen

Päätin lähteä tutkimaan opinnäytetyössä siviilitiedustelulainsäädännön vaikutuksia yritysten toimintaan. Tutkimuksen tavoitteena on selventää mitä käynnissä oleva siviilitiedustelulainsäädäntöhanke tarkoittaisi toteutuessaan yritysten liiketoiminnassa. Erityisen tarkastelun kohteena ovat tietointensiiviset yritykset sekä luottamuksellista tietoa liiketoiminnassaan hyödyntävät yritykset. Pohdin muun muassa kysymyksiä:

- Vaikuttaako käynnissä oleva hanke yritysten toimintaan millään tavalla?
- Onko mahdollisella lainsäädännöllä vaikutuksia kyseisten yritysten halukkuuteen investoida tulevaisuudessa Suomeen?
- Onko lainsäädännöllä vaikutusta esimerkiksi Suomessa käytävään kansainväliseen liiketoimintaan?
- Miten elinkeinoelämä kokee, että sitä on huomioitu käynnissä olevassa lakihankkeessa?
- Onko siviilitiedustelun hankkeella jotain erityisiä hyötyjä tai haittoja yritysten toiminnan kannalta?

Tutkimuskysymyksen kautta pyritään pureutumaan siihen, että millä tavoin Suomen kaltainen tietoyhteiskunta tai korkean teknologian yritykset joutuvat huomioimaan digitalisaation ja kyberympäristön muutokset omassa toiminnassaan, jotta toiminnan käytettävyys, sietokyky sekä varmuus, tehokkuus ja turvallisuus pystytään huomioimaan kokonaisuutena.

2.3 Rajaukset

Käynnissä oleva tiedustelulakihanke koostuu sotilas- ja siviilitiedustelulain kokonaisuudesta. Hanke on kokonaisuutena tarkastellen mittava ja tästä syystä ei käytännössä ole mahdollista käsitellä koko tiedustelulakikokonaisuutta kyseisessä tutkimuksessa. Kyseistä työtä on lähdetty rajaamaan erityisesti niistä syistä, että työn avulla olisi mahdollista saada uutta tietoa tällä

hetkellä varsin tuntemattomasta aihealueesta, joka koskettaa toteutuessaan laajasti suomalaista yhteiskuntaa, sen viranomaisia sekä suomalaista yritysmaailmaa.

Kyseinen tutkimus käsittelee käynnissä olevaa tiedustelulakihankekokonaisuutta siviilitiedustelun näkökulmasta, huomioiden erityisesti erikseen syntyvän tietoliikennetiedustelulain mahdolliset vaikutukset suomalaiseen elinkeinoelämään. Tarkastelun keskipisteessä on tietoliikennetiedusteluun olennaisesti liittyvän kyberturvallisuuden taso suomalaisissa yrityksissä. Vaikka asiaan liittyy myös esimerkiksi yksityisyyden suoja ja muut yksittäisille kansalaisille tärkeät asiat, niin työssä ei oteta tutkittavaksi lainsäädännön mahdollisia vaikutuksia kansalaisten yksityisyyden suojaan tai muuhunkaan, mikä koskettaa yksittäistä ihmistä.

Tutkimus ei ota kantaa siihen, millainen lainsäädäntö lopullisessa muodossaan on, vaan työssä tarkastellaan siviilitiedustelulain tarpeellisuutta, sen todennäköisiä vaikutuksia yritysten toimintaan ja investointihalukkuuteen sekä elinkeinoelämän roolia kansallisen turvallisuuden näkökulmasta. Työssä pyritään myös peilaamaan kyseistä lainsäädäntöhanketta muualla Euroopan maissa tapahtuvaan samankaltaiseen lainsäädäntökehitykseen.

Vaikka tiedustelulakien tarpeellisuudesta on erityisesti mediassa käyty vilkasta keskustelua, on se keskittynyt hyvin paljolti muun muassa terrorismintorjuntaan, tiedustelutoiminnan havaitsemiseen sekä yksityisyyden suojaan. Työssä ei käsitellä laajalti tiedustelulakikokonaisuuden tuomia toimivaltuussäädöksiä tai muutoksia turvallisuusviranomaisten näkökulmasta. Tarkoituksena on erityisesti korostaa hanketta yritysten nykyisen turvallisuusympäristön näkökulmasta huomioiden sen vaikutukset kyberturvallisuuteen sekä yritysten kykyyn suojata omia tietojansa.

2.4 Rakenne ja eteneminen

Tutkimus rakentuu kahdesta eri kokonaisuudesta. Ensinnäkin työssä pyritään kuvaamaan valmisteilla olevaa siviilitiedustelulainsäädäntöä ja tämän valmistelutyön aikana syntyneitä havaintoja varsin yritystoiminnan lähtökohdista. Lainsäädännön kannalta tutkimuksessa käsitellään erityisesti digitalisaation sekä tietoliikennetiedustelun mukanaan tuomia vaikutuksia suomalaisen yritysten toimintaan erityisesti yritysten tietopääoman suojaamisen ja nykyisen kyberturvallisuuden kannalta. Tarkoituksena ei kuitenkaan ole tehdä kattavaa katsausta lainsäädännön ja juridiikan näkökulmasta, vaan pitää keskiössä enemmänkin elinkeinoelämää ja yritysmaailmaa koskettavat osa-alueet.

Toiseksi tämä tutkimus pyrkii erityisesti suoritettujen asiantuntijahaastatteluiden myötä selventämään, miten käytännössä suomalaiset kyberturvallisuuden sekä tiedustelulainsäädäntöhanketta seuranneet asiantuntijat näkevät tulevan lainsäädännön todelliset vaikutukset yri-

tysten toiminnassa. Asiantuntijoiden näkemysten perusteella pyritään myös hahmottamaan yritysten nykyistä kyberturvallisuuden tasoa sekä millaisia vaikutuksia käynnissä olevalla tiedustelulainsäädäntöhankkeella olisi ulkomaisten investointien näkökulmasta.

Tutkimuksen rakenne on muodostettu niin, että se olisi mahdollisimman looginen ja helppolukuinen. Työn jakaminen tiedustelulainsäädännön kannalta keskeisiin kokonaisuuksiin sekä yritysten näkökulman eriyttäminen helpottavat kokonaisuuden hahmottamista ja tuloksiin perehtymistä.

3 Tutkimustarategia, tietoperusta, metodivalinta ja keskeiset käsitteet

Opinnäytetyön kohteena oleva aihealue on suomalaisessa tutkimuskentässä melko tuntematon kokonaisuus, joten työssä käytettävälle tutkimusmenetelmälle tai teoreettiselle viitekehykselle ei ollut olemassa suoranaista vertailupohjaa aiemmista tutkimuksista. Aihealuetta on käsitelty jonkin verran kansainvälisessä tutkimuksessa, mutta sen täysimittainen soveltaminen Suomessa käynnissä olevaan lainsäädäntöhankkeeseen tuntui vieraalta. Suoranaisesti käynnissä olevasta tiedustelulakihankkeesta on tehty Laurea-ammattikorkeakoulussa Niko Anttosen ja Janne Takkusen ylemmän ammattikorkeakoulun opinto-ohjelman jatkotutkimus, jossa pohditaan mahdollisia tiedustelulainsäädännön vaikutuksia suomalaisten turvallisuusviranomaisten näkökulmasta (Anttonen & Takkunen 2016).

Tiedustelulakihanke on suurelta osalta keskittynyt Suomen kansallisen turvallisuuden parantamiseen sekä siihen liittyvän uhka- ja tilannetiedon parantamiseen. Suurin osa käytössä olevista aikaisemmista tutkimuksistaja käydystä julkisesta keskustelusta onkin keskittynyt erityisesti turvallisuusviranomaisten toimintaan sekä niiden toimivaltuuksien oikeutukseen. Kuitenkin tässä työssä on tarkastelun kohteena lakihankkeen vaikutukset suomalaisen elinkeinoelämän ja yritysten kannalta. Tietoperusta näyttäytyikinalkuun ohuelta, osaksi jo pelkästään siitä syystä, ettei käynnissä oleva lainsäädäntöhankkeen sisältämiä lakimuutoksia ole hyväksytty eduskunnassa vuoden 2018 alussa.

Tutkimuksen kohteena olevasta aiheesta oli saatavilla varsin rajallisesti monipuolista aineistoa. Tästä syystä ratkaisuksi valittiin menettely, jossa ennen kaikkea suomalaisesta kirjallisuudesta löydettyjä tutkimustuloksia, dokumenttiaineistosta nousevaa tietoa sekä asiantuntijahaastatteluista saatua materiaalia käsitellään yhdessä. Tutkimuksessa nivotaan yhteen asiantuntijahaastattelujen ja teorian kautta saatua tietoa, mitä kuljetetaan suunnitellun rakenteen läpi koko työn. Tutkimuksen käytössä olevaa aineistoa käsitellään menetelmällisesti dokumenttianalyysin ja asianauntijahaastatteluiden avulla tutkimustehtävää palvelevan rakenteen mukaisesti.

3.1 Tutkimusstrategia

Tutkimus perustuu kvalitatiiviseen eli laadulliseen tutkimukseen, minkä lähtökohtana on todellisen elämän kuvaaminen. Laadulliseen tutkimukseen liittyy olennaisesti ajatus siitä, että todellisuus on moninainen ja sitä ei voi pirstoa haluamallaan tavalla osiin. Kokonaisuus koostuu toisiinsa monensuuntaisesti suhteissa olevista tapahtumista, jotka muovaavat toinen toisiaan samanaikaisesti. Laadullisessa tutkimuksessa pyritäänkin tutkimaan kohdetta mahdollisimman kokonaisvaltaisesti. (Hirsjärvi et al. 2009, 160-161.)

Yleisesti kvalitatiivisen tutkimuksen tyypillisenä piirteenä onkin se, että tutkimus on nähtävä kokonaisvaltaisena tiedon hankintana, jossa tietoperusta ja aineisto kootaan todellisissa tilanteissa. Useimmiten tiedon keruun instrumenttina suositaan ihmistä ja tutkija luottaa enemmän omiin havaintoihinsa ja keskusteluihin tutkittaviensa kanssa kuin erilaisissa mittausvälineillä hankittavaan tietoon. Laadullinen tutkimus pyrkii käyttämään hyväksi induktiivista päättelyä, mikä tarkoittaa sitä, että tutkijan tarkoituksena on paljastaa odottamattomia seikkoja, mitkä eivät ole yleisesti tiedossa. Tämän vuoksi tutkimuksen lähtökohtana ei olekaan teorian tai hypoteesien testaaminen vaan aineiston monipuolinen ja yksityiskohtainen tarkastelu. (Hirsjärvi et al. 2009, 164.)

Kvalitatiiviseen tutkimukseen kuuluu myös aineiston hankinnassa käytettävien laadullisten menetelmien käyttö. Tämä tarkoittaa käytännössä sitä, että suositaan sellaisia menetelmiä, joissa tutkittavien näkökulmat tulevat selkeästi esiin. Tällaisina menetelminä voidaan pitää muun muassa ryhmä- ja teemahaastatteluja, osallistuvaa havainnointia sekä erilaisten dokumenttien ja tekstien diskursiivisia analyyseja. Tutkimuksen kohdejoukko valitaan tarkoituksenmukaisesti, eikä satunnaisuutta käyttäen. Laadullisessa tutkimuksessa tutkimussuunnitelma muotoutuu osaksi tutkimuksen edetessä, mikä tarkoittaa sitä, että tutkimus tulee toteuttaa joustavasti sekä suunnitelmia täytyy pystyä muuttamaan olosuhteiden muuttuessa. (Hirsjärvi et al. 2009, 164.)

Yksi laadullisen tutkimuksen peruskulmakivistä, johon tutkimuksessa nojaudutaan liittyy havaintojen teoriapitoisuuteen. Edellä mainitulla teoriapitoisuudella tarkoitetaan, että millainen yksilön käsitys ilmiöstä on, millaisia merkityksiä tutkittavalle ilmiölle annetaan tai millaisia välineitä tutkimuksessa sekä sen edetessä käytetään. Tutkimusta tehtäessä myös ilmiön tarkastelun näkökulma vaikuttaa tutkimustyypin valintaan. Näiden näkökulmien ero on pelkistettävissä havaintoaineiston ja argumentaation väliseksi eroksi. Näin ollen on perusteltua puhua eri tutkimustyyppeihin sisältyvistä erilaisista analyysimuodoista, toisin sanoen teoreettisesta ja empiirisestä analyysista. (Tuomi & Sarajärvi 2012, 20.)

Havaintoaineiston tarkastelu sekä argumentointi eroavat empiirisessä ja teoreettisessa analyysissa kahdella tavalla. Empiirisessä analyysissa korostuvat erityisesti käytettävän aineiston

keruu- ja analyysimetodit. Tämä tarkoittaa sitä, että empiiristä tutkimusta ei voida ajatella ilman, ettei olisi selostettu aineiston keräämis- ja analyysimenetelmää. Näiden kuvaaminen antaa tutkimusta lukevalle mahdollisuuden arvioida tutkimusta ja se on oleellinen osa tulosten uskottavuutta. Teoreettiseen analyysiin ei sitä vastoin empiirisen analyysin tapaan ole varsinaista menetelmää. Teoreettisessa analyysissa on kyse enemmänkin eräänlaisesta ongelmanratkaisuesseestä. Teoreettisen tutkimuksen keskeinen uskottavuuskysymys keskittyy siihen, kuinka uskottavasti ja pätevästi lähdeaineistoa käytetään. (Tuomi & Sarajärvi 2012, 21.)

Tämä koostuu hyvin pitkälti empiirisestä analyysistä, johon liittyy oleellisena osana induktiivinen päättely. Tuomi ja Sarajärvi kirjoittavat kirjassaan, että aineistolähtöisen laadullisen eli induktiivisen aineiston analyysi voidaan karkeasti jakaa kolmevaiheiseksi prosessiksi: 1) aineiston pelkistäminen tai redusointi, 2) aineiston ryhmittely eli klusterointi ja 3) abstrahointi, jolla tarkoitetaan teoreettisten käsitteiden luomista. Aineiston pelkistämisessä analysoitava tieto tai data voi olla esimerkiksi aukikirjoitettu haastatteluaineisto tai muu asiakirja, joka pelkistetään siten, että aineistosta karsitaan tutkimukselle epäolennainen pois. Aineiston ryhmittelyn vaiheessa käytettävästä tiedosta etsitään samankaltaisuuksia tai eroavaisuuksia kuvaavia käsitteitä. Ryhmittelyn jälkeen seuraa aineiston abstrahointi, missä erotetaan tutkimuksen kannalta olennainen tieto ja valikoidun tiedon perusteella muodostetaan teoreettisia käsitteitä. (Tuomi & Sarajärvi 2012, 109-111.)

Dokumenttianalyysi on tapa lähestyä tutkimusta, missä kiinnostuksen kohteena olevaa tutkimusaineistoa ei ole koottu suorilla ja välittömillä havainnoilla. Dokumenttianalyysia voidaan käyttää myös toisella tutkimusmenetelmällä suoritettavan tutkimusaiheen esitutkintaan. Valmiit dokumentit voivat auttaa uuden ilmiön tutkimuksessa, sillä dokumenteista on mahdollista saada tietoa siitä, kuinka muut ovat menetelleet ja millaista tietoa aiheesta on saatavilla. Aineistona voi olla kirjeet, lehtikirjoitukset, päiväkirjat, omaelämänkerrat, lait tai esimerkiksi sopimukset. Tietyissä tutkimusaiheissa valmiin aineiston käyttäminen on ainoa tapa saada tietoa kyseisestä tutkimusalueesta. (Sivonen 2017, 17.)

Dokumenttianalyysin tavoitteena on järjestelmällinen aineiston läpikäynti ja analysointi sekä selkeän kuvauksen luominen tutkittavasta ilmiöstä. Aineistoa käsitellään loogisen päättelyn ja tulkinnan avulla. Dokumenttien analysoinnissa käytetään joko aineistolähtöistä sisältöanalyysia tai teorialähtöistä sisältöanalyysiä. Aineiston lähdekriittisyys vaatii tutkijalta huolellisuutta sitä enemmän mitä useamman portaan kautta tieto on siirtynyt eteenpäin. Dokumenttianalyysin heikkous on siinä, että aineisto voi olla alun perin luotu muuta tarkoitusta varten, eikä tutkija enää pysty vaikuttamaan siihen. (Sivonen 2017, 18.)

Asiantuntijahaastatteluiden toteuttaminen on moninainen prosessi, jossa haastattelun tekijä joutuu usein miettimään, miten määritellä oman tutkimusaiheensa näkökulmasta oleelliset

asiantuntijatahot sekä olennainen asiantuntijuuden taso. Hyvärinen et al. ovat määritelleet, että asiantuntijat ovat niitä henkilöitä, joiden tietämys tutkittavasta aiheesta on sellaista, mitä ei ole kelläkään muulla tai ainoastaan hyvin harvoilla. Usein asiantuntijahaastattelu perustuu johonkin teemaan eli se on puolistrukturoidun haastattelun muunnelma. (Hyvärinen et al. 2017, 182-186.)

Asiantuntijahaastattelu tuottaa kuitenkin vain rajallinen aineiston tuottamisen menetelmä. Haastatteluilla voi olla eri käyttötapoja, mutta keskenään erilaisia asiantuntijahaastatteluita yhdistää tavoite tuottaa uutta tietoa käyttämällä hyödyksi asiantuntijoiden erityistä tietämystä. Hyvärinen et al. mainitsevat kirjassaan kolme tapaa käyttää asiantuntijahaastattelua. Ensimmäinen tapa on eksploratiivinen haastattelu tai kartoittava asiantuntijahaastattelu. Tätä menetelmää sovelletaan usein vähän tutkittuun ilmiöön ja se on tutkijalle nopea tapa tutustua uuteen tutkimusaiheeseen. Toinen haastattelun tapa on käyttää systemaattista haastattelua, jolla pyritään kokonaisvaltaisesti hahmottamaan jonkin asiantuntijan mahdollisimman objektiivinen tieto. Kolmantena tapana voidaan käyttää teoriaa luovaa asiantuntijahaastattelua, missä pyritään asiantuntija objektiivisen tiedon lisäksi rekonstruoimaan myös piilevää tietoa asiantuntijan toiminnasta ja tulkinnosta. (Hyvärinen et al. 2017, 184.)

Asiantuntijahaastattelussa tulee huomioida, että asiantuntijalla saattaa olla pyrkimys vaikuttaa tutkimuksen lähestymistapaan. Erityisesti valtaa pitävät asiantuntijat saattavat kokea, että tutkimus uhkaa heidän etujaan tai mainettaan.Tämän vuoksi haastattelijan on hyvä osata vakuuttaa haastateltavat siitä, ettei haastatteluun osallistumisesta ole heille haittaa. (Hyvärinen et al. 2017, 191.)

Tarkoituksena on lähestyä tutkimuskysymystä laadullisen tutkimuksen kautta, missä aineistona käytetään muun muuassa yksilöhaastatteluiden sekä olemassa olevan kirjallisen dokumentaation pohjalta saatuja tietoja. Tutkimuksen pyrkimyksenä on tuoda esiin mahdollisia ennakkoon tuntemattomia seikkoja, jotka liittyvät tutkimusaiheeseen sekä tutkimuskysymykseen.

3.2 Lähteistä ja tutkimusaineistosta

Suomessa käynnissä olevasta tiedustelulakeihin liittyvästä lainsäädäntöhankkeesta tai siihen liittyvästä problematiikasta ei ollut juurikaan tutkimusta, vaan suuri osa materiaalista koostui median käsittelemistä aiheista julkisessa keskustelussa. Teoreettisesta näkökulmasta tarkasteltuna ministeriöiden eri työryhmien muodostamat esitykset, mietinnöt ja lausunnot muodostivat tosiasiallisen pohjan tämänkin tutkimuksen tietoperustalle. Erityisesti sisäministeriön vuonna 2015 asettaman siviilitiedustelulakityöryhmän mietintö, joka lopulta luovutettiin silloiselle sisäministerille Paula Risikolle 19.4.2017, toimi perustavanlaatuisena pohjana tälle tutkimukselle.

Opinnäytetyön tutkimusaineistona toimii pääasiallisesti toteutetut asiantuntijahaastattelut sekä lainsäädäntöhankkeen kannalta eri työvaiheiden keskeisin kirjallinen materiaali. Yhdeksi tärkeimmäksi dokumentiksi siviilitiedustelulainsäädäntötyön näkökulmasta hallituksen esitys siviilitiedustelulainsäädännöksi, mikä luovutettiin eduskunnalle 25.1.2018. Kyseisessä esityksessä ehdotetaan säädettäväksi kokonaan uusi laki tietoliikennetiedustelusta siviilitiedustelussa sekä muun muassa poliisilakia esitetään muutettavaksi siten, että siihen lisättäisiin uusi luku, jossa säädettäisiin tiedustelumenetelmistä ja niiden käytöstä siviilitiedustelussa (HE 202/2017 vp, 1). Lisäksi esityksessä ehdotetaan tehtäväksi erinäisiä muutoksia muihin keskeisiin lakeihin kuten rikoslakiin, esitutkinta- sekä pakkokeinolakeihin, lakiin poliisin hallinnosta ja lakiin henkilötietojen käsittelystä poliisitoimessa.

Tutkimuksen kirjallisina lähteenä käytetään myös sisäministeriön asettaman siviilitiedustelulakityöryhmän mietintöä 8/2017, joka luovutettiin silloiselle sisäministeri Paula Risikolle 19.4.2017. Aihealueen ollessa melko tuore tutkimuksen näkökulmasta koin tarpeellisena ottaa mukaan median näkökulmaa valmistelutyön aikana. Medialla on tämänkaltaisissa valmistelutöissä merkittävä rooli, sillä julkisessa keskustelussa tulee tuoda esille millaisia vaikutuksia kyseisellä lainsäädännöllä voisi toteutuessaan olla niin yksittäisille kansalaisille, kotimaiselle elinkeinoelämälle tai kansainvälistä toimintaa harjoittaville yrityksille. Mediassa käyty keskustelu kohdistui pitkälti yksityisyyden suojaan liittyviin kysymyksiin ja tästä syystä yritysten ja elinkeinoelämän rooli jäi melko pieneksi median näkökulmasta. Tästä syystä päädyin haastattelemaan suomalaisia tieto- ja kyberturvallisuuden asiantuntijoita tai lainsäädäntötyössä mukana olleita henkilöitä, jotta olisi mahdollista muodostaa hyvin moninainen sekä puolueeton näkemys siviilitiedustelulainsäädännöstä.

3.3 Haastattelujen toteutus

Koska tutkimuksen kohteena olevaa aihekokonaisuutta ja tutkimuskysymyksiä ei juurikaan ole käsitelty Suomessa, joten katsoin tarpeelliseksi hankkia aiheeseen liittyvää tietoa myös haastattelun keinoin. Opinnäytetyön aihetta varten muodostettiin haastattelurunko (liite 1), joka perustui haastattelutyyppinä teemahaastatteluun.Haastattelupyynnöt lähetettiin huhti-toukokuussa 2017 yhteensä kymmenelle henkilölle, jotka toimivat tietoturva- ja kyberturvallisuusalalla eri tehtävissä tai ovat olleet mukana tiedustelulakihankkeessa työtehtäviensä vuoksi. Pyynnöissä painotettiin, että tutkimukseen osallistuminen olisi täysin vapaaehtoista ja se voidaan keskeyttää milloin tahansa. Haastattelupyyntöihin vastasi kahdeksan henkilöä ja näiden henkilöiden haastattelut suoritettiin kesä-elokuun välisenä aikana. Teleoperaattorin edustaja ei vastannut haastattelupyyntöön. Haastateltaville lähetettiin noin viikkoa ennen haastattelua haastattelurunko, jonka avulla he pystyivät valmistautumaan haastatteluun. Jokainen haastattelu nauhoitettiin äänitallentimella haastateltavan suostumuksella, jotta haas-

tattelu pystyttiin litteroimaan jälkikäteen. Lähetetty yleinen haastatteluрunko löytyy tämän opinnäytetyön liitteistä.

Haastattelut suoritettiin joko haastateltavien työpaikoilla tai muun muassa kahviloissa. Lopulta haastatteluihin otti osaa yhdeksän henkilöä. Työn kannalta haastateltavien tarkka yksilöinti ei ole tarpeellista, joten päädyin luomaan haastelluista alla olevan listauksen. Listauksessa on mainittu kunkin haastattelun ajankohta sekä jokaiselle haastatellulle on luotu omanlainen alias, millä pyritään selventämään haastatellun roolia.

Toteutuneet haastattelut:

1. Kyberturvallisuusjohtaja, kansainvälinen asiantuntijayritys, haastattelu 17.5.2017
2. Professori, suomalainen yliopisto, haastattelu 24.5.2017
3. Viranomainen, turvallisuussektori, haastattelu 30.5.2017
4. Virkamies, lainsäädännön valmistelun näkökulma, haastattelu 2.6.2017
5. Tietoturvajohtaja, suomalainen asiantuntijayritys, haastattelu 9.6.2017
6. Yritysturvallisuuden asiantuntija, elinkeinoelämän näkökulma, haastattelu 14.6.2017
7. Turvallisuusjohtaja, kansainvälinen teknologiakonserni, haastattelu 19.6.2017
8. Kehitysjohtaja ja johtava tietoturvakonsultti, kyberturvallisuuspalveluita tarjoava yritys, haastattelu 11.8.2017

Tutkimushaastattelut on useimmiten tapana nauhoittaa käyttäen esimerkiksi äänitallenninta, mutta myös videotallennusta voidaan käyttää. Nauhoittaminen ei aina ole mahdollista ja joissakin tapauksissa tutkimustilanteen seuraaminen on helpompaa ilman nauhoitusta. Useissa haastatteluissa nauhoittamisesta on kuitenkin enemmän etua kuin haittaa. Tilanteen nauhoittaminen antaa tutkijalle mahdollisuuden tarkastella toisten tekemiä haastatteluita, koska tutkija ja haastattelija eivät aina välttämättä ole yksi ja sama henkilö. Haastattelun tallentaminen mahdollistaa myös tilanteeseen palaamisen uudelleen, koska tallenne toimii muistiapuna sekä tulkintojen tarkastamisen välineenä. (Ruusuvuori & Tiittula 2005, 14-15)

Nauhoituksen ansiosta haastattelusta voidaan raportoida tarkemmin. Tutkimusanalyysia varten tallennetut haastattelut on muutettava kirjoitettuun muotoon eli litteroitava. Litterointi on nähtävä hyvänä muistiapuna ja helpottaa tärkeiden yksityiskohtien löytämistä kokonaisaineistosta. Litteroinnin tarkkuus riippuu tutkimuksen kohteena olevasta tutkimuskysymyksistä ja käytetystä tutkimusmetodista. Haastatteluaineiston avulla tuotettua tietoa raportoitaessa on mietittävä tarkoin henkilöiden tunnistettavuuteen liittyviä kysymyksiä. Mikäli ihmisiä haastatellaan yksityishenkilöinä, on erityisen tärkeätä, ettei heidän henkilöllisyytensä käy ilmi raportista. Yksityisyyden suojaamiseksi henkilöiden nimet ja muut tunnistamista mahdollistavat tiedot muutetaan. (Ruusuvuori & Tiittula 2005, 16-17.)

3.4 Keskeiset käsitteet

Tutkimuksen tarkoituksena on käsitellä aihetta ja tutkimuskysymystä sekä pääkäsitteiden välisiä suhteita erityisesti siltä kannalta, että millä tavoin Suomen kaltainen tietoyhteiskunta pyrkii kehittämään ja suojaamaan tiedustelulainsäädännön kautta omia etujaan entistä digitalisoituvassa ja globalisoituvammassa, tietoverkkoihin, perustuvassa maailmassa. Tällä kehityksellä on väistämättä vaikutuksia erityisesti niihin yrityksiin, joiden liiketoiminta perustuu tiedon hyödyntämiseen liiketoiminnassaan. Opinnäytetyön aihetta käsiteltäessä törmätään väistämättä moneen eri osa-alueeseen, jotka muodostavat oleellisen osan tutkimuksen sisällöstä. Pyrin kuvaamaan näitä osa-alueita työssä käytettävien keskeisten käsitteiden avulla, minkä tarkoituksena on selkeyttää mistä asioista käynnissä oleva tiedustelulakihanke koostuu, millaisia vaikutuksia sillä mahdollisesti saattaa olla esimerkiksi yritystoiminnan kannalta sekä mitkä kokonaisuudet liittyvät oleellisilta osiltaan kyseiseen kokonaisuuteen.

Tänä päivänä keskustellaan paljon kyberturvallisuudesta, kyberistä tai kybertoimintaympäristöstä. Yhteiskuntamme monet toiminnot perustuvat digitaalisen maailman olemassaololle ja arkipäiväiset asiat kuten sähkön ja vedenjakelu ei olisi mahdollista ilman bittien olemassaoloa. Kuten Jarno Limnéll et al. kuvaavat Kyberturvallisuus-kirjassa, kyberillä tarkoitetaan digitaalista maailmaa, joka ympäröi meitä ja joka vaikuttaa meidän jokapäiväiseen elämäämme entistä voimakkaammin. Kyber rinnastetaan usein kybertoimintaympäristöön, mutta harvoin sitä käytetään yksittäisenä sanana. Kyber on nähtävä enemmänkin digitaalista maailmaa kuvaavana yhdyssanan etuliitteenä, kuten kyberturvallisuus, kyberrikollisuus tai kyberuhka. Kyberillä viitataan myös fyysisen ja digitaalisen maailman rajapintaan, kyberfyysiseen kokonaisuuteen, jossa elämme tällä hetkellä. Lisäksi Limnéllin et al. mukaan kyber on ennen kaikkea strateginen käsite, mikä yhdistää datan, informaation ja tiedon käytön osaksi kokonaisvaikutusta ja tuon vaikutuksen ohjailemista haluttuun suuntaan. Käytännössä tämä tarkoittaa sitä digitaalista maailmaa, josta koko nykymuotoinen yhteiskuntamme sekä liiketoimintamme ovat erittäin riippuvaisia. (Limnéll et al 2014, 28-29.)

Kyberturvallisuus itsessään ei ole välttämättä mikään uusi asia. Kyberturvallisuus tulisi nähdä tietokoneturvallisuutta, tietoverkkoturvallisuutta sekä tietoturvallisuutta laajempana ja kokonaisvaltaisempana käsitteenä. Tietyllä tavalla nämä kaikki osa-alueet liittyvät osaksi kyberturvallisuutta, mutta kyberturvallisuus pyrkii kattamaan alleen koko digitaalisen maailman turvallisuuskysymykset. Globaalissa mielessä kyberturvallisuudelle ei ole olemassa yhtä selkeätä määritelmää, mikä osaltaan vaikeuttaa kyberturvallisuuden kokonaisuuden konkreettista hahmottamista. Kyberturvallisuus-kirjan kirjoittajien mukaan kyberturvallisuus vaatii yhteistyötä, ajanmukaista tilannekuvaa, joustavia turvallisuustoimia sekä jatkuvaa turvallisuuskulttuurin kehittämistä (Limnéll et al. 2014, 20).

Tämän tutkimuksen kannalta tiedustelun ja erityisesti siviilitiedustelun selventäminen on omiaan havainnollistamaan minkälaisen sateenvarjokäsitteen alle nykyinen tiedustelulainsäädäntöhanke kuuluu. Sisäministeriön julkaisun 16/2017 mukaan tiedustelusta yleiskäsitteenä puhuttaessa tarkoitetaan sillä erilaisin menetelmin toteutettua tiedonhankintaa, jota suorittaa tätä varten organisoitu ja määrätty sekä näiden tiedustelumenetelmien käyttöön oikeutettu ja erikoistunut viranomainen tai muu taho. Tiedustelutoiminta eroaa tiedonhankinnasta muun muassa sillä, että kyse ei ole satunnaisesta tai yksittäisiin tietoihin keskittävästä tiedonhankinnasta. (Sisäministeriön julkaisu 16/2017, 11.)

Siviilitiedustelulla tarkoitetaan ensisijaisesti kansallisen turvallisuuden suojaamiseksi suoritettavaa valtion sisäisten ja ulkoisten turvallisuusuhkien tunnistamista, näihin uhkiin kohdistuvaa tiedonhankintaa, kyseisen tiedon analysointia sekä tämän kokonaisprosessin lopputuloksena saatavan tiedustelutiedon oikea-aikaista toimittamista sen tiedon tarvitsijoille. Siviili- ja sotilastiedustelun eroja tarkasteltaessa on muistettava, että usein näitä toimintoja suorittavat organisaatiot ovat usein eri sijainneissa valtiohallinnossa sekä niiden toimivalta ja tehtävät voivat poiketa toisistaan. Siviilitiedusteluorganisaatiot ovat siviiliviranomaisia ja pääsääntöisesti oman hallinnonalansa ministeriön ohjauksessa. Suomessa suojelupoliisia ollaan muuttamassa siviilitiedusteluviranomaiseksi, joka toimisi sisäministeriön ohjauksessa. (Sisäministeriön julkaisu 16/2017, 11.)

Sisäministeriön mukaan yksi keskeisimmistä tiedustelulainsäädäntöhankkeen tavoitteista on kansallisen turvallisuuden parantaminen. Hankkeen tavoitteena on myös valmistella siviilitiedustelua koskevat keskeiset säännökset ja tällä tavoin parantaa suojelupoliisin tiedonhankintamahdollisuuksia liittyen muun muassa kansallisen turvallisuuden parantamiseksi. Suomen lainsäädännössä kansallista turvallisuutta ei ole määritelty selkeästi. Tähän mennessä kansallisen turvallisuuden sijaan on viitattu muun muassa valtion sisäiseen ja ulkoiseen turvallisuuteen. Eduskunnassa tällä hetkellä olevien lainsäädäntömietintöjen ehdotuksissa on lähtökohtana se, että varsinaisen kansallisen turvallisuuden määrittelyn sijaan määritellään ne uhat kansalliselle turvallisuudelle, joiden havaitsemiseksi, tunnistamiseksi sekä joihin kohdistuvan tiedonhankinnan toteuttamiseksi voidaan käyttää erilaisia tiedusteluvaltuuksia. (Sisäministeriön julkaisu 16/2017, 12.)

Mietintöjen mukaan Suomen kansallista turvallisuutta uhkaavalla toiminnalla tarkoitetaan toimintaa, jota voidaan pitää haitallisena valtion keskeisille toiminnoille sekä eduille. Ilmaisu käsittää siis näin ollen sen, ettei uhkaavan toiminnan tarvitse ensisijaisesti kohdistua kehenkään yksilöön, vaan yleisemmin valtioon tai yhteiskuntaan. Kansallista turvallisuutta vakavasti uhkaava toiminta voi olla myös sellaista, joka toteutuessaan olisi rikos, mutta johon ei vielä voida kohdistaa konkreettista ja yksilöityä rikosepäilyä. Tämä tarkoittaa käytännössä niitä tilanteita, joissa on tarpeen havaita, selvittää sekä seurata, että johtaako jokin sinällään vie-

lä laillinen toiminta valtioon tai yhteiskuntajärjestykseen kohdistuvaan vakavaan rikokseen. Kansallisen turvallisuuden suojaamista on mahdollista ja tarpeellista tehdä useilla muillakin tavoin kuin tiedustelulainsäädännön kautta. Näitä tapoja voivat olla esimerkiksi ulko- ja turvallisuuspoliittinen päätöksenteko, varautuminen sekä viestintä ja ennaltaehkäisevä toiminta. Edellä mainituista tavoista vastaavat lukuisat toimijat yhteiskunnassa, mutta päävastuu painottuu valtion ylimpään johtoon ja muihin päätöksentekijöihin. (Sisäministeriön julkaisu 16/2017, 13.)

Tiedustelulainsäädäntöhankkeen yhtenä alullepanevana voimana on julkisessakin keskustelussa esitetty Suomen turvallisuusympäristön muutosta. Hallituksen esityksessä eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi mainitaan, että turvallisuusympäristö on monimutkaistunut ja näihin liittyvät haasteet sekä tehtävät edellyttävät viranomaisilta asianmukaista suorituskykyä. Turvallisuusympäristön muutoksiin on vastattava ajanmukaistamalla turvallisuusviranomaisten tilannekuvaa, toimivaltuuksia ja parantamalla eri viranomaisten suorituskykyä. Turvallisuusympäristömuutoksen uusien uhkien ilmenemismuotoja voivat olla muun muassa terrorismi sekä hybridi- ja kyberuhat, jotka voivat toimia myös voimapolitiikan välineinä. (HE 202/2017 vp, 9.)

Tutkimuksen yhtenä keskeisenä käsitteenä toimii siviilitiedustelulakihankkeessa kokonaan uutena lakina esitetty laki tietoliikennetiedustelusta siviilitiedustelussa. Käytännössä laissa tarkoitetun tietoliikennetiedustelun käyttäjänä olisi siviilitiedusteluviranomaisena toimiva suojelupoliisi. Yleistasolla tietoliikennetiedustelulla tarkoitetaan lakiesityksessä Suomen rajan viestintäverkossa ylittävään tietoliikenteeseen kohdistuvaa, automatisoituun erotteluun pohjautuvaa teknisesti suoritettua tiedonhankintaa sekä tällä tavoin hankitun tiedon käsittelyä. Tietoliikennetiedustelua voitaisiin kohdistaa siis vain sellaiseen tietoliikenteeseen, joka ylittäisi valtakunnanrajan siirtymällä suomalaisesta viestintäverkosta ulkomaiseen viestintäverkkoon tai päinvastoin. (HE 202/2017 vp, 122.)

Tietoliikennetiedustelun käyttö vaatisi aina tuomioistuimen luvan, mikä ratkaisisi asian suojelupoliisin päällikön kirjallisesta vaatimuksesta. Vaatimuksessa tulisi käydä ilmi yksityiskohtaisesti tietoliikennetiedustelun perusteena oleva kohde ja ne tosiseikat, joihin tietoliikennetiedustelun käytön edellytykset, muun muassa vakava uhka kansalliselle turvallisuudelle ja välttämättömyys, perustuisi. Tämän lisäksi tuomioistuimen myöntämä lupa edellyttäisi, että tuomioistuin vakuuttuisi suojelupoliisin esittämän aineiston perusteella edellä mainituista seikoista. (HE 202/2017 vp, 127.)

Tämän työn keskeinen tutkimuskysymys liittyy erityisesti siviilitiedustelulakihankkeessa käsitellyn tietoliikennetiedustelun mahdollisiin vaikutuksiin yritysten liiketoiminnassa. Tutkimuksessa suurin mielenkiinto kohdistuu tietointensiivisiin yrityksiin sekä näiden liiketoimintaa.

Tietointensiivisellä liiketoiminnalla tarkoitetaan yritystoimintaa, jossa liiketoiminnan kautta tuotettavien tuotteiden, palveluiden tai asiantuntijuuden tunnuspiirteenä on tiedon merkittävyys. Tieto voi näkyä liiketoiminnassa muun muassa tuotteiden ja tuotantoprosessien tietointensiivisyytenä, tieto voidaan nähdä työn raaka-aineena tai tieto voi olla työn tulos.

4 Käynnissä oleva tiedustelulainsäädäntöhanke

Käynnissä oleva tiedustelulakihanke sai alkunsa vuonna 2013, jolloin Puolustusministeriön alainen Turvallisuuskomitea julkaisi Suomen kyberturvallisuusstrategian, missä pohdittiin muun muassa lainsäädännön kehittämistä tiedonhankinnan sekä tiedustelun näkökulmasta (Turvallisuuskomitea 2013, 34-35). Loppuvuodesta 2013 Puolustusministeriön tiedonhankintalakityöryhmä ryhtyi pohtimaan turvallisuusviranomaisten tiedonhankintakyvyn parantamista erityisesti tietoverkkoympäristössä tapahtuvien vakavien uhkien ympärillä. Työryhmä julkaisi mietintönsä vuonna 2015 ja luovutti sen silloiselle puolustusministeri Carl Haglundille.

Tiedustelulainsäädännön valmistelu jatkui vuonna 2015 kolmessa erillisessä työryhmässä, joiden työtä valvoi sisäministeriön asettama parlamentaarinen seurantaryhmä. Hankkeen työnjako jakaantui siten, että sisäministeriö johti siviilitiedustelua koskevaa hanketta, puolustusministeriö sotilastiedustelua koskevaa hanketta sekä oikeusministeriö perustuslain mahdollista muuttamista koskevaa hanketta. Tiedustelulainsäädäntöhankkeeseen liittyy oleellisesti perustuslaillinen pohdinta ja tällä voi olla suuria vaikutuksia hankkeen aikatauluun ja näin ollen lain lopulliseen sisältöön. (Puolustusministeriö 2015c.)

Sisäministeriön siviilitiedustelulakityöryhmä luovutti mietintönsä sisäministeri Paula Risikolle alkuvuodesta 2017. Siviilitiedustelulakityöryhmän mietintö oli lausuntokierroksella 24.4.-16.6.2017 ja hallituksen esitys siviilitiedustelulainsäädännöstä luovutettiin eduskunnalle 25.1.2018 (Sisäministeriö 2018). Nykyinen hallitus haluaisi lakien tulevan voimaan vuonna 2019 päättyvällä hallituskaudella. Tällä hetkellä lakiesitysten säätäminen vaatii perustuslain muuttamista ja mikäli sitä halutaan kyseisen hallituskauden aikana, tulisi viisi kuudesosaa kansanedustajista kannattaa lakien säätämistä kiireellisenä. (Yleisradio 2018.)

4.1 Tiedustelutoiminnan toimivaltuudet

Heti hankkeen alusta lähtien kokonaisuus on jakanut niin viranomaisia, elinkeinoelämää kuin yksityisiä kansalaisiakin ja osin syystäkin. Erityisesti turvallisuusviranomaisten sekä osittain poliittisten toimijoiden näkökulmasta Suomi tarvitsee siviilitiedustelua kansallisen turvallisuuden suojaamiseen. Perimmäisenä tarkoituksena varsinkin sisäministeriöllä on ollut se, että kyseisellä lainsäädännöllä parannetaan suomalaisen yhteiskunnan mahdollisuuksia suojautua

kansalliseen turvallisuuteen kohdistuvilta vakavilta uhkilta. Tämänkaltaisia uhkia voivat olla esimerkiksi terrorismi, vieraiden valtioiden Suomeen kohdistama vakoilu tai elintärkeän infrastruktuurin lamauttaminen, missä elinkeinoelämällä on suuri rooli. Lainsäätäjän näkökulmasta tarvetta on perusteltu muun muassa Suomen turvallisuusympäristön nopealla muutoksella, joiden myötä uudet uhat edellyttävät uudenlaista valmiutta ja varautumista. Siviilitiedustelulainsäädännön tavoitteena on täten mahdollistaa tehokas tiedonsaanti näistä uhista ja tällä tavoin tukea valtion ylimmän johdon päätöksentekoa sekä varmistaa päätösten perustuminen oikeaan, ajantasaiseen sekä luotettavaan tietoon. (Sisäministeriö 2017.)

Haastatteluun osallistunut virkamies valotti asiaa, että tällä hetkellä viranomaisilla ei ole mahdollisuutta hankkia uhkaperusteista tietoa erityisesti niistä ilmiöistä, jotka muodostavat uhan kansalliselle turvallisuudelle. Nykyisellään toimivaltaisten viranomaisten tiedonhankinta perustuu vain avoimiin lähteisiin tai sitten ollaan ”ulkomaisen tiedusteluyhteistyön ja tiedusteluagentuurien hyväntahtoisuuden varassa”. Voimassa oleva lainsäädäntö, joka koskettaa erityisesti poliisia ja Suojelupoliisia perustuu siihen, että aina täytyy olla jokin tietty yksilöitävissä oleva henkilö, mihin kohdistetaan esimerkiksi erilaisia pakkokeinoja. Toimivaltuuksien käytössä pitää olla syytä olettaa, että tietty henkilö tietyllä todennäköisyydellä syyllistyy johonkin rikoslain tunnusmerkistön mukaiseen tekoon. Tämä teko täytyy pystyä myös yksilöimään ja on huomioitava myös muita edellytyksiä. Tiedonhankinta nykyisellään perustuu rikoskytkentään, joten ongelmat tällä hetkellä kulminoituvat siihen, että viranomaisilla tulee aina olla jokin rikosperuste sekä epäilty henkilö.

Toimivaltuuksien käytön perusteet aiheuttavat huomattavan ongelman tiedustelutoiminnan näkökulmasta, koska usein ei pystytä vielä tiedonhankintavaiheessa osoittamaan selkeää rikosepäilyä tai yksilöimään tiettyä henkilöä tähän epäilyyn. Suomessa tiedustelutoimintaa varten ei ole laissa säädettyjä toimivaltuuksia. Yhtenä keskeisenä piirteenä kansallisesta turvallisuudesta vastaavien viranomaisten tehtäville sekä toimille on, että ne koskettavat erilaisten uhkien torjuntaa. Tehokas uhkien torjunta edellyttää, että uhat pystytään havaitsemaan ja niistä saadaan riittävän varhain ajantasaista sekä mahdollisimman oikeata tietoa. Kansallisia uhkia torjuvien viranomaisten tiedustelutoimivaltuuksista ja näiden valtuuksien jakautumisesta sotilas- ja siviiliviranomaisten välillä ei ole säännelty. Kuten haastateltu virkamies kertoi, nykyisellään lainsäädännössä viranomaisten tiedonhankintaa koskettavat tiedonhankintatoimivaltuudet perustuvat tiedustelun sijaan yksinomaan rikostorjuntaan. Siviilitiedustelulakityöryhmän mukaan nykytilaa voidaan pitää epätyydyttävänä ottaen huomioon ne turvallisuusympäristön muutokset, joita viime aikoina on tapahtunut. Lainsäädännön tulee mahdollistaa erityisesti uhkaperusteisen tiedon hankkiminen, minkä avulla voidaan varautua erityisesti Suomen ulkoa käsin tapahtuvien uhkien ja tekojen torjuntaan. Tietoverkkojen välityksellä tai suoraan sitä kautta tapahtuvat uhat ovat yksi esimerkki muuttuneesta turvallisuusympäristöstä. (Sisäministeriön julkaisu 16/2017, 85-86.)

4.2 Tiedustelulakihankkeen ensiaskeleet

Puolustusministeriön tiedonhankintalakityöryhmä lähetti mietintönsä alkuvuodesta 2015 laajalle lausuntokierrokselle ja lausuntoa pyydettiin 150 eri ministeriöiltä, viranomaiselta, puolueelta, järjestöiltä ja yhteisöiltä sekä yrityksiltä. Lisäksi lausuntopyyntö lähetettiin eri alojen professoreille ja se oli julkisesti saatavilla puolustusministeriön internet-sivuilta. Lausuntopyyntöön tuli vastauksia yhteensä 74 kappaletta. Lausuntojen yhteinen palaute oli se, että nykyisellään digitalisoituva ja korkeasti tietoverkottunut yhteiskuntamme on toimintaympäristön muutoksessa. Ongelmallisena kuitenkin pidettiin viranomaisten tiedonsaantitarpeiden sekä yksityisyyden suojan välisen jännitteen yhteensovittamista. (Puolustusministeriö 2015, 3.)

Tiedustelulainsäädäntöhankkeen alkuvaiheessa hanke koki melkoista vastustusta erityisesti elinkeinoelämän suunnasta. Elinkeinoelämän keskusliiton (EK) mukaan suunniteltu tiedustelulaki vähentäisi sijoitusten ja erilaisten investointien Suomeen. EK mainitsi jo vuonna 2014, että lainvalmistelussa tulisi ottaa enemmän huomioon yritysten näkökulma, eikä edistää asiaa pelkästään turvallisuusviranomaisten näkökulmista. (Helsingin Sanomat 2014.)

Opinnäytetyöhön haastatellun yritysturvallisuuden asiantuntijan mielestä elinkeinoelämän vastustus johtui pitkälti siitä, ettei silloinen työryhmä ollut viestinyt selkeästi siitä vaatimuksia kohdennettaisiin yritysten suuntaan. Suurimmat kynnyskysymykset liittyivät mahdollisiin tietojärjestelmiin tehtävien takaporttien asentamiseen tai salausavainten luovuttamiseen viranomaisille. Lisäksi elinkeinoelämä koki, että sen läsnäolo olisi ollut suotavaa lakikokonaisuutta valmistelleessa puolustusministeriön asettamassa työryhmässä. Julkisessa keskustelussa puhuttiin myös massavalvonnasta, mikä omalta osaltaan aiheutti epätietoisuutta niin yritysten kuin kansalaistenkin keskuudessa. Myöhemmässä vaiheessa valmistelutyöryhmien toimesta tehtiin varsin selväksi, ettei yrityksiä velvoiteta luovuttamaan salausavaimia tai asentamaan takaportteja järjestelmiinsä. Lisäksi sisäministeriön vuonna 2015 tekemän siviilitiedustelun lainsäädäntövalmistelua koskevassa asettamispäätöksessä (Sisäministeriö 2015) yksiselitteisesti mainitaan, ettei yrityksiä velvoitettaisi asentamaan järjestelmiinsä tai palveluihinsa takaportteja tai luovuttamaan viranomaisille salausavaimia.

Vuodesta 2015 jatkuneessa lainvalmistelutyössä tämä kritiikki otettiin vastaan ja sitä lähdettiin kehittämään aktiivisesti. Sisäministeriön siviilitiedustelulakia valmistelleen työryhmän pysyväiseksi jäseneksi kutsuttiin Elinkeinoelämän keskusliiton yritysturvallisuuden johtava asiantuntija Mika Susi pyydettiin pysyväksi asiantuntijaksi työryhmään, jotta erityisesti elinkeinoelämän tarpeita voitaisiin huomioida paremmin kuin aiemmin työryhmän aikaan. Lisäksi tämän tutkimuksen haastatteluun osallistunut virkamies kertoi, että siviilitiedustelulakityöryhmä panosti huomattavasti valmistelutyön viestintään niin yritysten kuin mediankin suun-

taan ja tällä tavoin pyrittiin oikomaan sekä selventämään niitä väärinymmärryksiä, joita julkisessa keskustelussa oli aikanaan. Virkamiehen mukaan viestinnällä oli suuri merkitys siinä, että valmistelutyön aikana tiedustelulainsäädäntöhankkeessa alettiin nähdä enemmän positiivisia puolia kuin negatiivisia.

Siviilitiedustelulakityöryhmän luovutettua mietintönsä silloiselle sisäministeri Paula Risikolle 19.4.2017 muun muassa eräät järjestöt sekä elinkeinoelämä kannatti tiedustelulakihanketta. EK:n mukaan Suomessa on tarvetta siviili- ja sotilastiedustelun lainsäädännölle pelkästään senkin takia, että nykyinen tilanne on varsin epäselvä. Aiemmin myös negatiivisina riskeinä nähdyt vaikutukset Suomeen tehtäville sijoituksille hälvenivät valmistelutyön edetessä. (Tekniikka & talous 2017.)

Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry piti myös tärkeänä, että tiedusteluun liittyviä toimivaltuuksia sekä yritysten vastuita tähän liittyen selkeytetään. FiCom lausui asiassa, että se pitää tiedustelusäädäntökokonaisuuden lähtökohtia hyväksyttävinä, mutta koska kyseessä on mittava kokonaisuus, tulee kokonaisuus analysoida tarkasti. (FiCom 2017.) Finnish Information Security Cluster ry FISC, joka koostuu noin 70 keskisuuresta tieto- ja kyberturvaan keskittyvästä yrityksestä oli tiiviisti mukana lakien valmistelutyössä EK:n koordinoiman tiedustelulakien seurantaryhmän kautta. FISC:n mukaan elinkeinoelämän kannalta lainsäädännön kannalta on tärkeätä huomioida hyvä yrityssalaisuuden suoja, viranomaisten ja elinkeinoelämän yhteistyö turvallisuusuhkien torjunnassa sekä nopeasti kehittyvä teknologia ja sen rooli. Tietoturvakonsortion mukaan tiedustelulainsäädäntöä tarvitaan Suomessa, mutta on tärkeätä etteivät uudistuvat toimivaltuudet aiheuta elinkeinoelämälle kustannuksia tai heikennä yritysten kilpailukykyä saati toimintamahdollisuuksia. (FISC 2017.)

4.3 Siviilitiedustelulainsäädäntöhankkeen yleiskuvaus

Tiedustelulakin tarpeellisuudesta on Suomessa keskusteltu pitkään. Muualla maailmassa tiedustelulla on olennainen rooli niin kansallisen turvallisuuden kuin erilaisten kansallisten intressien näkökulmasta. Suomessa lainsäädännön arvellaan olevan tässä mielessä noin 15 vuotta jäljessä. Erityisesti Euroopassa viime vuosina tapahtuneen terroristi-iskut ovat vauhdittaneet osaltaan keskustelua tiedustelulakien tarpeellisuudesta. Hankkeen puolestapuhujat uskovat, että tarpeellisilla toimivaltuuksilla voitaisiin estää mahdollisia uusia terrori-iskuja tai vieraiden valtioiden harjoittamaa vakoilutoimintaa Suomessa. Hanketta vastustavat tahot eivät puolestaan usko siviilitiedustelulakien myötä tulevien tiedonhankintamenetelmien tehokkuuteen sellaisenaan ja lainsäädännön vaatima perustuslain muutoksen kiirehtiminen aiheuttaa epäluuloa. (Keskisuomalainen 2016.)

Suomessa ei ole tällä hetkellä voimassaolevaa lainsäädäntö liittyen sotilas- tai siviilitiedusteluun sekä lisäksi tiedustelua ja sen eri osa-alueita kuvaava käsitteistö on pitkälti vakiintumatonta sekä tulkinnanvaraista. Puolustusministeriön työryhmä määritteli vuonna 2015 siviilitiedustelun siviiliviranomaisen suorittamaksi tiedusteluksi, jolla pyritään tuottamaan tietoa ylimmän valtionjohdon päätöksenteon ja oman operatiivisen toiminnan tueksi muista kuin sotilaallisen maanpuolustuksen alaan liittyvistä aiheista. Siviilitiedustelu poikkeaa poliisin rikostorjunnassa suorittamasta rikostiedustelussa siten, että rikostiedustelun tarkoituksena on hankkia rikoksen estämisen, paljastamisen tai selvittämisen kannalta merkityksellistä tietoa rikollisista, rikoksista sekä rikoksenteko-olosuhteista. (Puolustusministeriö 2015, 16.)

Tähän työhön tehtyjen haastattelujen perusteella ei voida selkeästi vain yhtä alullepanevaa voimaa tiedustelulakihankkeelle. Haastateltujen asiantuntijoiden mielestä suurimpina vaikuttumina voidaan pitää toimintaympäristön muutosta, digitalisaatiota, hybridivaikuttamisen olemassaoloa sekä kybermaailman hyödyntämistä viimeaikaisissa sotilaallisissa operaatioissa. Keskeisenä tarpeena on nykypäivänä ajantasaisen uhkatiedon sekä tilannekuvan hankkiminen, jotta viranomaiset ja valtion johto saa näkyvyyttä sellaisista hankkeista tai ilmiöistä, mitkä saattavat vaarantaa tai muodostaa uhan Suomen kansalliselle turvallisuudelle. Tällä hetkellä nämä tiedonhankintamahdollisuudet ovat rikosperusteisia ja eivät mahdollista tiedon hankkimista tehokkaasti ulkomailta. Haastatellun kyberturvallisuusjohtajan mukaan yhtenä kiihdyttimenä tiedustelulakihankkeessa voidaan pitää ulkoministeriöön kohdistunutta tietomurtoa, joka tuli ilmi vuonna 2013.

Kyseisen tietovuodon todellisella merkityksellä nykyiselle lainsäädäntöhankkeelle ei ole tarkkaa tietoa, mutta se kertoo hyvin miten turvallisuusympäristö on muuttunut ja millaisia turvallisuusuhkia digitalisoitunut yhteiskunta aiheuttaa valtion johtamisen tasolla. Ulkoministeriössä paljastui vuonna 2013 laaja verkkovakoilutapaus, jonka seurauksena ministeriöstä vuoti huomattava määrä tietoja tuntemattomille tahoille. Vakoilutapaus paljastui tammikuussa 2013, kun Ruotsin signaalitiedustelulaitos Försvarets Radioanstalt (FRA) ilmoitti asiasta Suomen viranomaisille. (Tietoviikko 2014.) Suojelupoliisi tutki tietomurto törkeänä vakoiluna ja ulkomaisten tiedusteluelinten epäillään vakoilleen ulkoministeriötä ja vieneen tietoja. Tapauksesta ei ole tiedotettu julkisuuteen, mutta yleisesti epäillään, että useat eri tunkeutujat ovat toimineet ministeriön verkoissa jo vuosia. Tämä tapaus osoitti selkeästi Suomen nykytilanteen tiedustelullisesta näkökulmasta. Suomi on tällä hetkellä pitkälti ulkoisten yhteistyökumppaneiden sekä sidosryhmien hyvän tahdon kohteena. (Helsingin Sanomat 2013.)

Tutkimusta varten haastatellun professorin mielestä poliittinen ymmärrys tiedustelupuolen asioihin on Suomessa vielä aika heikkoa. Hän uskoo, että yksittäiset tapahtumat, kuten ulkoministeriön tapaus, voivat vauhdittaa lainsäädännön tarvetta yleisellä tasolla, mutta ennemmin syynä lainsäädännön tarpeella on vahva digitalisaatio ja sen korostuminen suhteessa fyy-

siseen maailmaan. Entistä enemmän rikoksia tehdään sekä tiedustelutoimintaa harjoitetaan kyberympäristössä ja tätä varten Suomeen on saatava selkeä lainsäädäntö. Nykyinen yhteiskuntamme on entistä riippuvaisempi digitaalisesta ympäristöstä ja mikäli Suomi, tai siellä toimivat yritykset, haluaa olla turvallinen ja kilpailukykyinen valtio, niin ei ole oikein muuta vaihtoehtoa kuin parantaa toimintaedellytyksiä kyberympäristössä.

Hallituksen esityksessä (HE 202/2017 vp) eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi mainitaan, että Suomen turvallisuusympäristö on merkittävästi muuttunut sekä digitalisoitunut ja tästä syystä sisäisen sekä ulkoisen turvallisuuden uhat limittyvät yhä tiiviimmin toisiinsa. Kansalliseen turvallisuuteen kohdistuvat vakavimmat uhat ovat lähes poikkeuksetta ulkomaista alkuperää tai niillä on selviä kytköksiä Suomen ulkopuolelle. Kansainvälistymisestä seuraa, että uhkien taustalla olevat tahot voivat olla verkostoituneita eri maiden alueille ja toimintaan osallistuvat tahot viestivät yli valtiorajojen. Viestintäteknologian nopea kehitys on tehostanut ja helpottanut Suomelle uhan muodostavien tahojen välistä maan rajat ylittävää yhteydenpitoa ja verkostoitumista sekä nopeuttanut yleisesti uhkien kansainvälistymistä. Digitalisaation myötä tietoverkoissa toteuttavia hyökkäyksiä voidaan käyttää niin poliittisen kuin taloudellisen painostuksen välineinä ja vakavissa kriiseissä yhtenä vaikuttamiskeinona sotilaallisten voimakeinojen ohella.

Alaluvussa 4.3.1 käsitellään lyhyesti siviilitiedustelulakikokonaisuuden kannalta oleellisimpia muutoksia viranomaisten toimivaltuuksien näkökulmasta sekä erityisesti Suojelupoliisin roolin muutosta turvallisuuskentässä.

4.3.1 Siviilitiedustelulainsäädännön tarpeet, tavoitteet ja hyödyt

Käynnissä olevalla tiedustelulainsäädäntöhankkeella voidaan arvioida olevan monia tarpeita sekä hyötyjä niin kansallisen turvallisuuden kuin yleisestikin yhteiskunnan näkökulmista. Kuten aiemmin tässä työssä on mainittu, niin Suomesta puuttuu tällä hetkellä erityisesti valtion ja yhteiskunnan toiminnan sekä turvallisuuden uhkaan liittyvän tiedonhankinnan lainsäädäntö. Kyseisillä tiedonhankintakyvykkyyksillä voitaisiin tuottaa valtion johdolle ajantasaista ja luotettavaa tilanne- ja uhkaperustaista tietoa, millä puolestaan voitaisiin taata mahdollisimman oikea-aikainen sekä tarkka päätöksenteko sitä tarvittaessa.

Hallituksen esityksessä (202/2017) määritellään selkeiksi siviilitiedustelulainsäädännön tarpeiksi alati muuttuva kansainvälinen turvallisuusympäristö sekä kehittyvä digitalisaatio ja hybridivaikuttaminen. Näistä syistä Suomen on kyettävä entistä tehokkaammin hankkimaan ajantasaista tietoa juuri ilmiö- ja uhkaperusteisesti. Tällä hetkellä voimassaolevilla rikostorjuntaan säädetyillä toimivaltuuksilla ei pystytä tehokkaasti sekä riittävän aikaisessa vaiheessa havaitsemaan yhteiskunnan turvallisuutta vaarantavia uhkia ja tarvittaessa estää niitä. Tieto-

liikennetiedustelun erityistavoitteena olisi parantaa Suomen mahdollisuuksia suojautua vakavimpien tietoverkkouhkien muodostamien turvallisuusriskien toteutumiselta. Esityksessä mainitaan, että tietoliikennetiedustelun kautta voidaan merkittävästi parantaa viranomaisten kykyä havaita erityisesti sellaisia kehittyneitä haittaohjelmia, joiden taustalla voidaan olettaa olevan valtiollisia toimia ja jotka saattavat aiheuttaa merkittävän uhan erityisesti yhteiskunnan kriittiselle infrastruktuurille tai valtion keskeisille toiminnoille.

Lainsäädäntöhanketta vastustetaan, mutta myös sen puolesta löytyy vahvaa kannatusta. Lainsäädäntöä valmistelleiden työryhmien avoimuus ja tehokas viestintä sai aikaan sen, että aiemmin hanketta vastustaneet tahot ovatkin kääntyneet viime aikoina hankkeen puolelle. Yhtenä esimerkkinä on Vihreiden kansanedustaja Jyrki Kasvi, joka alun perin vastusti lakihanketta, mutta on sittemmin muuttanut suhtautumistaan liittyen tiedustelulainsäädäntöön sekä sen tarpeellisuuteen. Kasvin mukaan Suomi on Euroopan ainoa maa, jossa siviili- ja sotilastiedustelua ei säädetä lailla. Eri maiden tiedusteluviranomaisten kanssa suoritettava tietojenvaihto sekä yhteistyö tarvitsee selkeitä pelisääntöjä. Lisäksi turvallisuusympäristö on muuttunut, josta esimerkkeinä Kasvi mainitsee sotilaallisen viestinnän siirtyneen paljolti radioaalloilla tietoverkkoihin, rikolliset ja terroristit ovat myöskin siirtyneet osittain tietoverkkoihin sekä Suomeen kohdistetaan ulkovaltojen tiedustelutoimintaan, mihin Suomella ei ole tällä hetkellä tehokkaita torjuntakeinoja. (Kasvi 2017.)

Turvallisuusympäristön muuttumisesta löytyy lähihistorista esimerkkejä, joista sotatieteen tohtori Saara Jantunen kirjoittaa Infosota-kirjassaan. Jantusen mukaan Ukrainan kriisin myötä suomalaiset havahtuivat pohtimaan, että onko Suomen turvallisuuspoliittinen tilanne muuttunut. Krimin miehityksen aikana havaittiin miten hybridisodankäyntiä hyödynnettiin osana perinteistä sodankäyntiä. Hybridisodankäynissä uutta sekä merkittävää eivät suinkaan olleet keinot tai niiden käyttäminen, vaan se missä roolissa informaatio- ja psykologinen vaikuttaminen olivat. Krimillä ja Itä-Ukrainassa nähdyssä hyökkäyksessä perinteisen kineettisen voimankäytön sijaan keskeisiä keinoja olivat erilaiset suostutteln ja painostuksen keinot. (Jantunen 2016, 28-29.)

Nykyisessä kybertoimintaympäristössä korostuu hybridisodankäynnissäkin havaittu attribuutio-ongelma, mikä liittyy erityisesti epäsymmetrisiin keinoihin. Usein on mahdotonta sanoa, että kuka todellisuudessa on esimerkiksi kyberhyökkäyksen takana. Samainen attribuutio-ongelma aiheuttaa haasteita myös informaatiosodankäynnin kannalta. Vaikka tietäisimmekin, että kyberhyökkäyksen takana olisi eräitä valtiollisia toimijoita, niin usein vastapuoli tulee vetoamaan todistamisvelvollisuuteen, mikä puolestaan on hyvin hankalaa puolustajan näkökulmasta. (Jantunen 2016, 58.)

Käynnissä olevalla lainsäädännöllä on vaikutuksia sekä hyötyjä myös muiden kuin viranomaisten ja valtion johdon kannalta. Yhteiskunnan turvallisuusstrategia on valtioneuvoston periaatepäätös, mikä julkistettiin vuonna 2017. Kyseisen periaatepäätöksen tarkoituksena on yhtenäistää poikkeustilanteisiin varautumisen kansallisia periaatteita ja ohjata erityisesti hallinnonalojen varautumista. Strategian mukaan kansallisen turvallisuuden voidaan katsoa käsittävän myös yhteiskunnan taloudellisten intressien turvaamisen. Elinkeinoelämän rooli varautumisessa on yhä tärkeämpi. Yrityksillä on jatkossakin keskeinen asema erityisesti talouden ja infrastruktuurin toimivuuden varmistamisessa. Lisäksi yritysten rooli esimerkiksi sosiaali- ja terveydenhuollon palveluiden tuottamisessa kasvaa. Pelkästään jo näistä syistä elinkeinoelämän roolin kasvun seurauksena on entistä tärkeämpää turvata yritysten oman toiminnan jatkuvuus. (Turvallisuuskomitea 2017, 10.)

Tässä mielessä elinkeinoelämän toimintaedellytysten ylläpito ja toimintavarmuus kuuluu osaltaan myös viranomaisten toimintakenttään. Toki suurin vastuu kuuluu elinkeinoelämälle ja yrityksille, joiden ensisijaisena tehtävänä on huolehtia omien toimintamahdollisuuksien olemassaolosta sekä toimintojensa kokonaisvaltaisesta turvaamisesta.

Tutkimukseen haastatellun yritysturvallisuuden asiantuntijan mukaan Suomessa on nykypäivänä hyvin vaikeata erottaa valtionhallintoa ja yksityistä sektoria toisistaan. Yksityinen sektori tuottaa merkittävän määrän yhteiskunnan kriittisistä palveluista, jopa suurimman osan. Nykyisellään yritysten ja elinkeinoelämän rooli ylipäätänsä yhteiskunnassa on hyvin merkittävä. Asiantuntija korostaakin, että lainsäädäntöä luotaessa yritysten rooli on muistettava tarkasti. Turvallisuuslähtökohdista perusteltu tilannekuvan parantuminen on tärkeätä ja se palvelee laajasti koko yhteiskuntaa, mukaan lukien yrityksiä. Yritysten liiketoiminnan näkökulmasta toimiva lainsäädäntö parantaa toimintaympäristöä ja turvallisuus paranee Suomessa. Toisaalta lainsäädännössä on huomioitava, että yritysten avustamisvelvollisuuteen linkittyy myös korvausmekanismi, jottei yrityksille aiheudu kustannuksia viranomaisten vaatimusten suhteen. Tämän mekanismin olemassaolo löytyy jo tällä hetkellä muun muassa pakkokeinolaista, jossa teleyrityksille myönnetään korvauksia telepakkokeinoihin nähden. Aiheutuneiden korvausten korvaaminen olisi hyvin perusteltua ja oikeudenmukaista sekä osaltaan kannustaisi yrityksiä myös tehokkaampaan yhteistyöhön. Kyseessä ei kuitenkaan tulisi olla mikään ansaintakeino yrityksille.

Siviilitiedustelulainsäädännön valmistelussa on pyritty huomioimaan hankkeen mahdolliset vaikutukset myös kansantalouden, yritysten sekä elinkeinoelämän kannalta. Hallituksen esityksen (202/2017) mukaan siviilitiedustelulainsäädännön tarkoituksena on suojata Suomen kansallista turvallisuutta, johon kansantalous oleellisena osana kuuluu. Tehokkaan tiedustelulainsäädännön kehittämisen arvioidaan nostavan ulkovaltojen suorittaman, osin taloudellisista lähtökohdista tapahtuvan, vakoilun kynnystä sekä estää tietoverkkojen kautta suoritettavaa

muuta haitallista toimintaa. Esityksessä korostetaan kuitenkin, ettei kyvykkyyden kasvattaminen poista tai vähennä yritysten, muiden yhteisöjen tai yksilöiden omien suojaustoimenpiteiden tarvetta. Elinkeinoelämän kannalta lainsäädännön selkeänä hyötynä kuvataan Suomen digitaalisen ympäristön turvallisuuden parantamista, mikä puolestaan edistää yritysten ja elinkeinoelämän suojautumismahdollisuuksia muun muassa yritysvakoilua vastaan. Esityksessä mainitaan, että tiedustelumenetelmien käytöllä saatuja tietoja voitaisiin tarvittaessa luovuttaa yrityksille vakavien uhkien torjumiseksi tai tärkeiden taloudellisten etujen puolustamiseksi.

Sisäministeriön työryhmän mukaan yhteiskuntaan kohdistuvien uhkien tunnistaminen ja siihen liittyvä torjunta sekä kriittisen infrastruktuurin ja valtion taloudellisen elinkelpoisuuden säilyttäminen edellyttävät yhteistyötä julkisen ja yksityisen sektorin toimijoiden välillä. Tässä suhteessa erityisen tärkeäksi muodostuu tiedusteluviranomaisten sujuva tietojen vaihto yritysten suuntaan toiminnan niin mahdollistaessa. Tästä syystä on oleellista säätää myös oikeusperusta sille, että suojelupoliisilla on mahdollisuudet luovuttaa tietoa yrityksille näiden merkittävien etujen suojaamiseksi. Tiedustelullisin keinoin tuotettua tietoa voitaisiin tarvittaessa luovuttaa yksityisille yhteisöille vakavien uhkien torjumisen mahdollistamiseksi tai merkittävien taloudellisten tappioiden estämiseksi. (Sisäministeriön julkaisu 8/2017, 165.)

4.3.2 Siviilitiedustelun tuomat muutokset

Sisäministeriön alaisen siviilitiedustelulakityöryhmän mukaan nykyistä lainsäädäntöä on kehitettävä siihen suuntaan, että viranomaisilla on entistä paremmat mahdollisuudet hankkia ilmiö- ja uhkaperustaista tietoa. Nykyisillä rikostorjuntatoimivaltuuksilla ei kyetä tarpeeksi varhaisessa vaiheessa havaitsemaan yhteiskunnan näkökulmasta sen turvallisuutta merkittävästi vaarantavia uhkia eikä näin ollen pystytä aloittamaan tarpeellisia toimenpiteitä näiden uhkien vaatimiin toimiin. Hallituksen esityksessä (HE 202/2017 vp) siviilitiedustelulakikokonaisuuden keskeiseksi tavoitteeksi määritellään kansallisen turvallisuuden parantaminen. Ehdotettavan lainsäädännön tavoitteena on myös tukea valtion ylimmän johdon päätöksentekokykyä ja varmistaa käytössä olevan tiedon oikeellisuus, ajantasaisuus sekä luotettavuus. Nykyisten turvallisuusviranomaisten toimintamahdollisuuksia sekä toimivaltuuksia tulee myös kehittää. Kyseisellä lainsäädännöllä mahdollistettaisiin suojelupoliisin sekä muiden kansallisen turvallisuuden viranomaisten ryhmien edellä mainittujen uhkien torjuntaan tarpeeksi aikaisessa vaiheessa.. Lisäksi suojelupoliisin tiedonhankintamahdollisuuksia parannettaisiin siten, että suojelupoliisilla olisi todelliset mahdollisuudet suoriutua sille määritellyistä tehtävistä, ottaen huomioon myös kansainväliset uhat.

Sisäministeriön työryhmä ehdotti mietinnössään, että Suomeen luotaisiin säädöspohja tietoliikennetiedustelulle, ulkomaan henkilötiedustelulle ja ulkomaantietojärjestelmätiedustelulle.

Samoista lähtökohdista olisi välttämätöntä luoda oma säädöspohja Suomessa käytettäville tiedustelutoimivaltuuksille kuin ulkomaan tiedustelullekin. Vakavimmat Suomeen kohdistuvat uhat ovat todennäköisimmin ulkomaisista lähteistä tulevia, voi tällaiset uhat toteutua myös Suomessa. Työryhmän mietinnön mukaan siviilitiedustelulainsäädännön keskeisin ydin koostuisi säädettävästä poliisilain 5 a luvusta, jossa määriteltäisiin perussäännökset tiedustelusta ja itse tiedustelumenetelmistä. Toinen merkittävä osuus säädettävän lainsäädännön kannalta olisi laki tietoliikennetiedustelusta siviilitiedustelussa. Siviilitiedustelulainsäädäntöön liittyy samanaikaisesti oleellisena osana puolustusministeriön johdolla tehtävä sotilastiedustelulainsäädännön valmistelu, oikeusministeriön valmistelema laki tiedustelun valvonnasta sekä eduskunnassa valmisteltava lakikokonaisuuden parlamentaarinen valvonta.

Hallituksen esityksen (HE 202/2017 vp) mukaan myös ulkomaan tiedustelutoimivaltuuksien ohella olisi tarpeen luoda säädöspohja kotimaassa käytettävistä tiedustelutoimivaltuuksista. Esityksen mukaan kokonaan uusi poliisilain 5 a luku (siviilitiedustelu) sisältäisi suojelupoliisin toimivallan puitteissa olevat tiedustelumenetelmät, joiden käytön perusteena olisi tiedonhankinta kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Poliisilain 5 a luvun tiedustelumenetelmiä olisivat hyvin pitkälti jo voimassa olevan poliisilain 5 luvun mukaiset sekä ne olisivat voimassa sekä kotimaassa, että ulkomailla. Säädettävät tiedustelumenetelmät olisivat:

- paikkatiedustelu, jäljentäminen sekä lähetyksen pysäyttäminen jäljentämistä varten (uudet toimivaltuudet)
- tietoliikennetiedustelu (uusi)
- telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta ja tukiasematietojen hankkiminen
- suunnitelmallinen tarkkailu ja peitelty tiedonhankinta
- tekninen tarkkailu, joka pitäisi sisällään teknisen kuuntelun, teknisen katselun, teknisen seurannan ja teknisen laitetarkkailun
- teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen
- peitetoiminta ja valeosto
- ohjattu tietolähdetoiminta

Kyseisen esityksen mukaan tuomioistuin päättäisi telekuuntelusta, televalvonnasta, tukiasematietojen hankkimisesta, teknisestä tarkkailusta ja paikkatiedustelusta tietyiltä osin sekä tietoliikennetiedustelun käytöstä kotimaassa. Suojelupoliisin päällikkö päättäisi ulkomaan tiedustelumenetelmien käytöstä.

Siviilitiedustelulakityöryhmä ehdotti mietinnössään, että suojelupoliisin tiedustelullisten toimivaltuuksien lisääntymisen myötä sen esitutkinta- ja pakkokeinotoimivaltuuksia tulisi rajoit-

taa oikeudenmukaisen oikeudenkäynnin turvaamiseksi. Tästä syystä työryhmä ehdotti, ettei suojelupoliisi olisi jatkossa esitutkintaviranomainen. Hallituksen esityksessä on mainittu myös, että sääntelyn tarkoituksena olisi korostaa sitä, että suojelupoliisi olisi ainoa viranomainen, jolla olisi oikeus käyttää poliisilain 5 a luvussa säädettyjä tiedustelumenetelmiä ja täten hankkia kyseisillä toimivaltuuksilla tietoa kansallista turvallisuutta uhkaavasta toiminnasta. Siviilitiedustelulla ja tiedustelumenetelmillä mahdollistettaisiin suojelupoliisin riittävän tehokas tiedonhankintakyky yhteiskunnan kannalta vakavimmista uhista, ilmiöistä sekä hankkeista.

Hallituksen esityksessä esitetään säädettäväksi kokonaan uusi laki, joka koskisi tietoliikennetiedustelua (laki tietoliikennetiedustelusta siviilitiedustelussa). Mainitun esityksen mukaan kyseessä olisi ainoastaan suojelupoliisin toimivallassa suoritettavaa tiedustelua. Tämän lisäksi määriteltäisiin erikseen tietoliikennetiedustelun käytöstä sotilastiedustelussa sekä tietoliikennetiedustelun teknisestä toteuttamisesta (sotilastiedustelulaki). Tietoliikennetiedustelun sisältöä tarkastellaan tarkemmin aihetta käsittelevässä luvussa 5.

Tehtyjen haastateltujen perusteella asiantuntijoiden yksimielinen kanta oli, että Suomeen tarvitaan selkeät pelisäännöt tiedustelun toteuttamiselle ja tiedustelumenetelmien säätämiselle on selkeä tarve. Haastateltu tietoturvallisuusjohtaja korostaa kuitenkin, että lainsäädäntö itsessään ei vielä paranna yleistä turvallisuutta, vaan tarvitaan käytännössä toimivia keinoja. Turvallisuussektorin virkamiehen mukaan suuri osa tiedosta liikkuu tälläkin hetkellä jo tietoverkoissa, joten viranomaisilla tulee olla selkeät mahdollisuudet suorittaa tiedonhankintaa myös siellä. Opinnäytetyön haastatteluihin osallistuneet kyberturvallisuusjohtaja, kyberturvallisuuspalveluita tarjoavan yrityksen asiantuntijat sekä tietoturvajohtaja olivat yhtä mieltä siitä, että Suomessa tulee seurata muita Euroopan maita tiedusteluun liittyen toimivaltuuksien kehittymisessä. Kyberturvallisuusjohtaja piti välttämättömänä tietoverkoissa tapahtuvan havaintokyvyn parantamista, koska nykyisellään löytyy useita viitteitä siitä, että suomalaisissa tietoverkoissa tapahtuu niin valtiollisten kuin järjestäytyneen rikollisuuden toimijoiden suorittamaan tiedonhankintaa sekä tietomurtoja.

4.3.3 Siviilitiedustelulakikokonaisuuden valvonta

Käynnissä oleva tiedustelulakihanke on herättänyt aktiivista keskustelua säädettävien tiedonhankintamenetelmien ja niitä käyttävien viranomaisten valvonnasta. Kyseisillä menetelmillä voi olla selkeitä liittymäpintojen yksilöiden nauttimaan yksityisyyden suojaan muun muassa käytettävien tiedonhankintamenetelmien kautta. Sisäministeriön työryhmä suoritti kattavan pohdinnan, jossa suuressa roolissa olivat muun muassa Suomen perustuslain sekä erilaisten velvoittavien kansainvälisten ihmisoikeussopimusten rajoitteet tiedustelutoiminnalle.

Nykyisellään tiedustelulakien läpivienti vaatisi muutoksia perustuslakiin ja siinä viestisalaisuuden rajoittamista koskevaan säädökseen. Perustuslain 10. pykälässä säädetään yksityiselämän suojasta ja luottamuksellisen viestin suojasta, mitkä ilmentävät hyvin Suomen korkeaa tietosuojaa yksilönkin kannalta. Oikeusministeriössä on valmisteltu perustuslain muutosta siten, että luottamuksellisen viestin salaisuuden rajoittamiseen tulisi lisäys. Nykyisellään perustuslaki sisältää maininnan välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta tai kotirauhaa vaarantavien rikosten torjunnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana koskevissa tapauksissa. Muissa tapauksissa luottamuksellisen viestin salaisuutta ei ole voitu rajoittaa. Kyseisten tiedustelulakien myötä edellä mainittuun listaan ehdotetaan lisättäväksi kohdat tiedon hankkimiseksi sotilaallisesta toiminnasta tai sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Lausuntokierroksella olleen esityksen sekä perustuslain muuttamisen tarpeellisuudesta ollaan melko yhtä mieltä, mutta poliittisella tasolla erityisesti erimielisyyttä syntyy siitä, että onko perustuslain muutoksia tarve säätää kiireellisinä tämän hallituskauden aikana. (Verkkouutiset 2018.)

Kuten yllä on nähtävissä, niin tiedustelulainsäädäntö tarvitsee myös uskottavan ja käytännössä toimivan laillisuusvalvonnan. Sisäministeriön siviilitiedustelulakityöryhmän mietinnön mukaan toiminnan valvontaan tuleekin panostaa. Hallituksen esityksen (202/2017) mukaan tiedustelun valvonta toteutettaisiin niin viranomais- kuin parlamentaarisin keinoin. Tiedustelutoiminnan viranomaisvalvontaan esitetään perustettavaksi riippumaton oikeudellinen valvoja, josta käytetään nimitystä tiedusteluvaltuutettu. Valtuutetun tehtävänä olisi valvoa viranomaisten suorittamaan tiedustelutoimintaa reaaliajassa. Lisäksi suojelupoliisin toiminnan valvontaa tehostettaisiin tiedusteluvaltuutetun toimesta. Suojelupoliisi olisi velvollinen antamaan tiedusteluvaltuutetulle tiedon tiedustelumenetelmää koskevasta luvasta tai suojelupoliisin päällikön tekemästä päätöksestä mahdollisimman pian. Tiedusteluvaltuutetulla olisi myös tosiasiallinen mahdollisuus keskeyttää tiedustelutoimivaltuuksien käyttö, mikäli se huomaisi toiminnassa joitakin voimassa olevan lainsäädännön vastaisia toimia. Tiedusteluvaltuutetulla olisi myös mahdollisuus päästä seuraamaan Helsingin käräjäoikeuden istuntoja, kun suojelupoliisi esittelee tiedustelutoimivaltuuksien käyttöön liittyviä vaatimuksiaan.

Poliisilain 5 a luvun mukaisia tiedustelumenetelmiä sekä tietoliikennetiedustelua koskevia lupavaatimuksia käsiteltäisiin sisäministeriön työryhmän mietinnön mukaan Helsingin käräjäoikeudessa. Tuomioistuinkäsittely keskitettäisiin Helsinkiin, koska käräjäoikeudella on muutenkin Suomen laajin kokemus salaisten tiedonhankinta-asioiden käsittelystä ja säädettävien toimivaltuuksien myöntäminen ja valvonta vaatii erikoisosaamista myös tuomioistuinten kannalta.

Hallituksen esityksessä (HE 202/2017 vp) myötäillään Euroopan ihmisoikeustuomioistuimen (EIT) kantaa siitä, että tiedustelun valvontaan osallistuisivat myös parlamentaarinen edustus. Sisäministeriön työryhmän mietinnön sekä hallituksen esityksen mukaan tiedustelutoiminnan parlamentaarisesta valvonnasta vastaisi kokonaan uusi tiedusteluvalvontavaliokunta. Valiokunta toimisi osana nykyistä eduskunnan valiokuntalaitosta. Tiedusteluvalvontavaliokunnalla olisi tehtävänsä hoitamiseksi tiedonsaantioikeuksien lisäksi oikeus saada tiedusteluvaltuutetulta ja muilta viranomaisilta tarvittavia selvityksiä.

Yllä esitettyjen valvontamekanismien lisäksi tiedustelutoimintaa voisi valvoa omien toimivaltuuksiensa puitteissa myös valtioneuvoston oikeuskansleri, eduskunnan oikeusasiamies sekä tietosuojavaltuutettu. Oikeusasiamies sekä oikeuskansleri ovat arvostelleet käynnissä olevan tiedustelulakien ehdotuksia erityisesti toiminnan valvonnan kannalta. Eduskunnan oikeusasiamiehen mukaan lainsäädäntöesityksissä mainittu kansallinen turvallisuus on käsitteenä epätäsmällinen ja tiedustelumenetelmien käytön edellytykset ovat hyvin väljiä verrattuna siihen, millä ehdoilla esitutkintaviranomaiset saavat käyttää samankaltaisia salaisia tiedonhankintakeinoja rikostutkinnassa. Oikeusasiamies on arvostellut valmistelutyötä siitä, että tuomioistuinten päätöstoimivaltaa tulisi tiedustelutoiminnassa korostaa, koska tällä hetkellä suojelupoliisin päällikölle tai puolustusvoimien tiedustelupäällikölle on tulossa merkittäviä lisävaltuuksia päättää tiedustelumenetelmien käytöstä. Oikeuskanslerinvirasto puolestaan kiinnitti lausunnossaan huomiota muun muassa siihen, että siviili- ja sotilastiedustelun välinen suhde tietoliikennetiedustelussa ja muussakin tiedustelussa jää varsin epämääräiseksi.

Lainsäädäntötyössä mukana olleen virkamiehen mukaan tehokas valvonta justifioi tiedustelutoiminnan. Ilman valvontaa voi toki olla tiedustelua, mutta oikeusvaltiossa ei voi olla tiedustelua tai tiedustelutoimivaltuuksia ilman tehokasta valvontaa. Euroopan ihmisoikeustuomioistuin on ratkaisukäytännössään viitoittanut paljon sitä, että pitää olla täysin riippumaton, tehokas sekä riittävän uskottava laillisuusvalvonta. Hänen mukaansa ehdotettu parlamentaarinen valvonta ei tule missään vaiheessa olemaan operatiivisen tason valvontaa, vaan tämä kuuluisi ulkoisen laillisuusvalvonnan eli tiedusteluvaltuutetun tehtäviin. Haastatellun professorin mukaan valvonnan kattavuudesta tarvitaan kokemusta, jota saadaan vasta siinä vaiheessa, kun lainsäädäntö tulee voimaan. Tärkeätä on varmistaa, että yritysten sekä kansalaisten luottamus säilyy suhteessa viranomaisten toimintaan. Yritysturvallisuuden asiantuntijan mukaan tiedustelutoiminnan valvonnalla on keskeinen rooli koko lainsäädännön uskottavuuden kannalta. Huomioitavaa on myös se, että ulkoisesti pitää pystyä osoittamaan, että lainsäädännöllä myös valvotaan toimintaa selkeästi ja avoimesti.

Sisäministeriön siviilitiedustelulakityöryhmä lähetti lausuntopyynnön mietinnöstään 96 taholle, mistä saatiin lopulta vastaus 65 taholta. Suurin osa lausunnonantajista piti uutta tiedustelulainsäädäntöä ja kokonaisuudesta säätämistä tarpeellisena sekä kannatettavana. Lausun-

nonantajien vähemmistö suhtautui mietintöön kriittisesti. Lausunnoissa painottuivat jonkin verran tietyt osa-alueet, kuten esimerkiksi mietinnön vaikutukset sekä perustuslakia koskevat osiot. Erityinen mielenkiinto lakiehdotuksissa kohdistui siviilitiedustelun kohteisiin, tietojen luovuttamiseen rikostorjuntaan sekä tietoliikennetiedustelua koskevaan lakiehdotukseen. (Sisäministeriön julkaisu 21/2017, 5.)

Tiedustelulainsäädäntö sai osin kriittistäkin palautetta. Yhtenä kritiikin antajana oli Suomessa kansalaisten sähköisiä oikeuksia puolustamaan perustettu Electronic Frontier Finland ry (Effi), joka antoi vuonna 2017 lausuntonsa sisäministeriön työryhmän ehdotukseen siviilitiedustelulaiksi. Effi:n mukaan erityisesti tietoliikennetiedustelun käytön edellytykset on määritelty liian epäselvästi. Lausunnossa nostettiin esiin myös tietoliikennetiedustelun mahdollisuus massavalvontaan, johon liittyvä kielto tulisi lisätä perustuslakiin. (Effi 2017.)

Luku 5 käsittelee uutta tietoliikennetiedustelua sekä sen mahdollisia vaikutuksia yritysten toimintaan. Kyseiseen aihealueeseen liittyy oleellisena osana nopeasti yhteiskunnassa etenevä digitalisaatio sekä kyberturvallisuus. Pyrin selvittämään tuleeko tiedustelumenetelmänä suunnitellulla tietoliikennetiedustelulla olemaan vaikutuksia yritysten kyberturvallisuuden näkökulmasta tai millaisia uhkia yritykset tänä päivänä kohtaavat tietoverkoissa.

5 Tietoliikennetiedustelu käytännössä

Anni Oittinen on maisteritutkielmassaan kuvannut yrityssalaisuuksiin kohdistuvia loukkauksia sekä kyberrikollisuutta yleisesti. Tutkielmassa on sivuttu myös tiedustelulainsäädäntöhanketta sen vaikutuksia yritysten toimintaan. Kansainvälinen kybertoimintaympäristö on muuttanut yritysten toimintaa entistä reaaliaikaisemmaksi ja tiiviimmäksi. Kehitys on toki lisännyt hyvinvointia, mutta tuonut mukanaan myös uusia uhkia, joista tietoverkkojen kautta tapahtuva kybervakoilu on yksi esimerkki. Kybervakoilu on erittäin kustannustehokas sekä alhaisen operaatioriskin sisältävä tiedonhankintakeino, millä voidaan saada suuria määriä luottamuksellista ja salassa pidettävää tietoa. (Oittinen 2017, 38.)

Puolustusministeriön tiedonhankintalakityöryhmän vuonna 2015 esitetyn mietinnössä mainitaan, että suomalaisiin kansantaloudellista merkitystä omaaviin yrityksiin kohdistuu jatkuvasti laajaa sekä teknisesti edistynyttä kybervakoilua. Vakoilutoimintaa voidaan kohdistaa myös tietojärjestelmiin, jotka sisältävät yrityssalaisuuksiksi luokiteltua tietoa. Tämänkaltaisen vakoilun tekovälineinä ei olisi kaupallisilla antivirusohjelmistoilla havaittavat haittaohjelmat, vaan tietoteknisesti kehittynyt sekä monipuolinen verkkohyökkäystyökalu, jonka tehtävänä olisi ensiksi tietyn tietoverkon osan ottaminen haltuun ja tämän jälkeen kehittyneempien hyökkäyksellisten vakoilu- sekä haittaohjelmien asentaminen. Kybervakoiluun liittyvät operaatiot on usein hyvin kohdistettuja ja tarkoin suunniteltuja, mikä kertoo valtiollisten toimi-

joiden toiminnasta. Vakoiluohjelmien lisäksi tietojärjestelmiin voidaan toimittaa haittaohjelmia, jotka aktivoituvat valtioiden välisen kriisin puhjettua. Kybertoimintaympäristössä tapahtuva vakoilu voi jatkua jopa vuosia ilman, että sitä havaitaan. (Oittinen 2017, 38.)

5.1 Laki tietoliikennetiedustelusta siviilitiedustelussa

Suurimpia muutoksia siviilitiedustelulainsäädäntöhankkeessa on kokonaan uuden toimivaltuuden, tietoliikennetiedustelun, säätämisestä. Kyseessä on melko monitahoinen, yksityiskohtainen ja osin haastava kokonaisuus. Tietoliikennetiedustelulla tarkoitetaan yksinkertaistettuna Suomen rajan viestintäverkossa ylittävään tietoliikenteeseen kohdistuvaa, lähtökohtaisesti tietoliikenteen automatisoituun erotteluun perustuvaa teknistä tiedonhankintaa sekä tämän kautta hankitun tiedon käsittelyä. (Knape 2017.)

Lain tarkoittaman tietoliikennetiedustelun käyttäjänä olisi suojelupoliisina, joka toimisi siviilitiedusteluviranomaisena. Kansallista turvallisuutta vakavasti uhkaavat toiminnat, mistä suojelupoliisilla olisi mahdollisuus hankkia tietoa käyttäen tietoliikennetiedustelua, olisi tyhjentävästi lueteltu laissa. Tietoliikennetiedustelun käytön perusteena olisi tietojen hankkiminen 1) terrorismista, 2) ulkomaisesta tiedustelutoiminnasta, 3) valtio- ja yhteiskuntajärjestystä uhkaavasta toiminnasta, 4) joukkotuhoaseista, 5) kaksikäyttötuotteiden kansallista turvallisuutta vakavasti uhkaavasta leviämisestä, 6) suuren ihmismäärän henkeä tai terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaavasta toiminnasta, 7) vieraan valtion suunnitelmasta tai toiminnasta, joka voisi aiheuttaa vahinkoa ulko- ja turvallisuuspolitiikalle tai kansainvälisille suhteille, taloudellisille tai muille tärkeille eduille, 8) kansainvälistä rauhaa ja turvallisuutta uhkaavasta kriisistä, 9) kansainvälistä kriisinhallintaoperaatiota uhkaavasta toiminnasta ja 10) kansallista turvallisuutta vakavasti uhkaavasta kansainvälisestä järjestäytyneestä rikollisuudesta. (Sisäministeriön julkaisu 8/2017, 138.)

Yllä mainittujen tietoliikennetiedustelun perusteuhkien on nähty olevan linjassa Euroopan ihmisoikeustuomioistuimen tulkintaan kansallisen turvallisuuden käsitettä tarkasteltaessa. Kyseiset uhat ovat kauttaaltaan niin vakavia, että ne voivat vaarantaa olemassa olevan valtiojärjestyksen tai yhteiskunnan perustoiminnot. Uhkien määrittelyssä on myös pyritty huomioimaan täsmällisyys, kuten kansainvälinen tuomioistuinkäytäntö edellyttää. (Sisäministeriön julkaisu 8/2017, 138.)

Hallituksen esityksen (202/2017) tietoliikennetiedustelun yleiskuvauksessa todetaan, että tietoliikennetiedustelu koskisi ainoastaan ja vain sellaista tietoliikennettä, joka ylittäisi valtakunnanrajan siirtymällä suomalaisesta viestintäverkosta ulkomaiseen viestintäverkkoon tai päinvastoin. Tämän määritellyn mukaan huomattava osa suomalaisesta tietoliikenteestä olisi jo tällä rajauksella tietoliikennetiedustelun ulkopuolelle. Esityksen mukaan viestintäverkon

määritelmään liittyisi vaatimus tiedonsiirron sähkömagneettisesta toteutuksesta, mutta muulla tavoin tiedonsiirto olisi teknologianeutraali. Valtaosa Suomen ja muiden maiden välisestä tietoliikenteestä välittyy muun muassa valokuitukaapeleissa, joten tästä syystä pääasiallinen tietoliikennetiedustelu kohdistuisi kaapelien kautta tapahtuvaan liikennöintiin. Tiedonsiirron teknologianeutraalisuudella varmistettaisiin se, että laki soveltuu käytettäväksi myös muissa teknisissä ympäristöissä ja muuttuvien viestintäteknologioiden olosuhteissa.

Menetelmällisesti tietoliikennetiedustelu perustuisi hallituksen tekemän esityksen (202/2017) mukaan tietoliikenteen automatisoituun erotteluun. Tällä menettelyllä toimivaltuus eroaisi muista sähköiseen viestintään kohdistuvista tiedonhankintamenetelmistä kuten telekuuntelusta ja -valvonnasta. Kyse ei siis olisi yksittäiseen tiedossa olevaan teleosoitteeseen tai telepäätelaitteeseen kohdistuvasta tiedonhankinnasta, vaan automaattisin menetelmien tapahtuvasta tietoliikenteen suodattamisesta niissä kohdin viestintäverkkoa, jonka kautta selvitettävänä olevaan uhkaan liittyvän tietoliikenteen voidaan olettaa kulkevan. Tietoliikennetiedustelu mahdollistaisi tiettyyn uhkaan liittyvän viestinnän havaitsemisen sekä sen taustalla olevien tahojen tunnistamisen ja paikallistamisen.

Kyseisen tiedustelumenetelmän käyttö ei mahdollista kaiken tietoliikenteen suodattamista, mikä ylittää Suomen rajan viestintäverkossa. Tietoliikennetiedustelun käyttö edellyttäisi, että suojelupoliisilla oli tieto tai epäilys jonkin yllä mainitun perusteuhkan konkreettisesta olemassaolosta ja tähän liittyvistä tosiseikoista. Rajan ylittävä viestintäverkon osa, jossa kulkevaan tietoliikenteeseen kyseisiä hakuehtoja saataisiin kohdistaa, tulisi mainita suojelupoliisin lupavaatimuksessa sekä tuomioistuimen lupapäätöksessä. Näin ollen hakuehtoja ei saisi käyttää muissa kuin tuomioistuimen lupapäätöksessä mainituissa viestintäverkon osissa siellä liikkuvaan tietoliikenteeseen. Lisäksi tietoliikennetiedustelun käytännön toteutuksesta säädettäisiin erikseen. (HE 202/2017 vp.)

5.2 Tietoliikennetiedustelun käytännön toteutus

Puolustusvoimien asettama tiedonhankintalakityöryhmä pohti mietinnössään vuonna 2015 tietoliikennetiedustelun käytännön toteutusta. Ryhmän mukaan ei ole tarkoituksenmukaista, että ne viranomaiset, jotka erityisesti tarvitsisivat tietoverkkojen kautta saatavaa tiedustelutietoa suorittaisivat tietoliikennetiedustelua kukin omillaan. Tätä tarvetta varten ryhmän mukaan tulisi luoda keskitetty ratkaisu, jossa tietoliikennetiedustelun teknisestä toteuttamisesta vastaisi yksi viranomainen (tietoliikennetiedusteluviranomainen). Viranomainen hankkisi muiden tietoliikennetiedustelutoimivaltuuden käyttöön oikeutettujen viranomaisten (toimeksiantajaviranomaiset) toimeksiannosta niiden tarvitsemat tietoliikennetiedot. (Puolustusministeriö 2015b, 66.)

Sisäministeriön siviilikakityöryhmän mietintö (Sisäministeriön julkaisu 8/2017) sekä hallituksen esitys (HE 202/2017 vp) ovat luopuneet tietoliikennetiedustelu- ja toimeksiantoviranomaisten määrittelystä, mutta keskitetystä ratkaisusta halutaan edelleen pitää kiinni. Esityksen mukaan puolustusvoimien tiedustelulaitos määrättäisiin lain tasolla suojelupoliisin tietoliikennetiedustelun tekniseksi toteuttajaksi. Suojelupoliisi määrittelisi tarkasti tuomioistuimelle tehtävässä lupavaatimuksessa ne tosiseikat, joiden perusteella tiedustelumenetelmän käyttöä anotaan sekä tietyt ja tarkat hakuehdot, joilla tietoliikenteen analysointi sekä suodatus toteutettaisiin.

Tietoliikennetiedustelun toteuttaminen edellyttäisi, että viestintäverkon valtakunnanrajan ylittävään osaan olisi ennalta toteutettu liityntäpinnat. Näiden liityntäpintojen rakentaminen tehtäisiin niiden yritysten myötävaikutuksella, jotka omistavat tai hallitsevat verkon rajan ylittävää osaa. Tuomioistuimelta saadun luvan myöntämisen jälkeen viestintäverkon osaan tehtäisiin kytkentä. Kytkennän suorittajana ja luvanmukaisena tietoliikenteen luovuttajana olisi Suomen Erillisverkot Oy. Tämä taho olisi valikoitunut sen vuoksi, että kyseessä olisi tiedusteluviranomaisista riippumaton taho, millä varmistettaisiin se, ettei viranomaiset saa laajempaa pääsyä tietoliikenteeseen kuin mitä tuomioistuimen myöntämä lupa mahdollistaa. Toimintaa valvoisi lisäksi tiedusteluvaltuutettu. Kytkennän kautta saatava tietoliikenne peilattaisiin puolustusvoimien tiedustelulaitoksen hallinnoiman tiedustelujärjestelmän läpi. Puolustusvoimat toimittaisi tuomioistuimen lupapäätöksessä määriteltyjen hakuehtojen mukaisen tietoliikenteen suojelupoliisille. (Sisäministeriön julkaisu 8/2017, 139-140.)

Hallituksen esityksen (HE 202/2017 vp) mukaan tietoliikennetiedustelun luonteesta johtuen tietoverkoissa liikkuvaan tietoliikenteeseen voidaan kohdistaa erilaisia hakuehtoja tarvittavan tiedustelutiedon saamiseksi. Siviilitiedustelulain esityksen mukaan suojelupoliisi muodostaisi tietoliikennetiedustelussa käytettävät hakuehdot tuomioistuimen hyväksymän hakuehtojen luokan rajoissa. Tällä menettelyllä varmistettaisiin se, että tiedusteluviranomainen ei pysty suodattamaan tietoverkoista kaikkea liikennettä. Lisäksi luottamuksellisen viestin sisältöä kuvaavan hakuehdon käyttö olisi tietoliikennetiedustelussa täysin kiellettyä. Hakuehdot eivät myöskään saisi sisältää henkilöiden nimi- tai muita yksilöintitietoja, eikä viestin semanttiseen sisältöön kuuluvia ilmaisuja.

Puolustusvoimien tiedustelujärjestelmään olisi ennalta määritelty tuomioistuimen kussakin lupapäätöksessä hyväksytyt hakuehdot, joihin järjestelmä vertaisi sen läpi virtaavaa tietoliikennettä automatisoidusti. Lakiehdotuksen mukaan sallittuja hakuehtoja olisivat, poislukien luottamuksellisen viestin semanttista sisältöä kuvaavat tiedot, tietoliikenteen ohjaus- ja välitystiedot eli käytännössä tietoverkolle tai tietojärjestelmälle tarkoitetut ohjeet, komennot tai muut metatiedot, millä vaikutetaan viestin kuljetukseen ja ohjaamiseen viestintäverkossa

ja tietojärjestelmässä. Lisäksi sallittuina hakuehtoina olisivat esimerkiksi tiedot jonkin salausohjelman tai aakkosmerkistön käytöstä. (HE 202/2017 vp.)

Siviilikäkityöryhmän tekemän mietinnön mukaan tietoliikennetiedustelusta säätäneiden vertailuvaltioiden (Ruotsi, Ranska, Yhdistynyt Kuningaskunta, Kanada, Saksa, Alankomaat, Sveitsi ja Suomi) lainsäädännössä ei ole asetettu samantyyppisiä rajoituksia tai esteitä käyttää sisällöllisiä hakuehtoja, vaan poiketen esitetystä niiden käyttö on kyseisissä maissa laajasti sallittu. Ryhmän mietinnön mukaan hakuehtojen hyväksymiseen perustuvan lupamenettely täyttäisi Euroopan ihmisoikeussopimuksen vaatimukset. Esimerkiksi Sveitsin tiedustelulakia muodostettaessa on huomioitu Euroopan ihmisoikeustuomioistuimen uusin ratkaisukäytäntö. (Sisäministeriön julkaisu 8/2017, 140.)

Haastatellun kyberturvallisuuspalveluita tarjoavan yrityksen kehitysjohtaja sekä johtaja tietoturvakonsultti olivat sitä mieltä, että käytettävien hakuehtojen suhteen tulee olla tarkkarajainen lainsäädäntö. Käytännössä tietoliikenteestä voidaan kyseisten hakuehtojen perusteella suorittaa tarkkaakin käyttäjän profilointi muun muassa käytettävän merkistön suhteen. Suomessa tilanne on melko vakaa, mutta lainsäädännön tulisi huomioida, että riippumatta mahdollisesta poliittisen ilmapiirin muutoksesta ei saisi syntyä tilannetta, jossa tietoliikennetiedustelua alettaisiin soveltamaan esimerkiksi etniseen seulontaan.

5.3 Yritysten velvollisuudet sekä tuomioistuimen päätöksenteko

Suomen rajan ylittävä viestintäverkko on yksityisten yritysten omistuksessa. Käytännössä valtionrajat ylittäviä datakaapeleita lähtee Suomesta Ruotsin ja Saksan suuntaan. Yksityisestä omistuspohjasta johtuen tietoliikennetiedustelun käytännön toteutus edellyttäisi muun muassa operaattoreita velvoittavan lainsäädännön säätämistä, jotta tietoliikennetiedustelua voidaan todellisuudessa toteuttaa. Tiedustelua ei voida toteuttaa, mikäli verkoissa kulkevaa liikennettä ei saada ohjattua yksityisen toimijan tietoverkosta puolustusvoimien tiedustelulaitoksen järjestelmän lävitse.

Siviilikäkityöryhmän mietinnön mukaan yllä mainittujen velvollisuuksien kohteena olevista tahoista käytettäisiin määritelmää tiedonsiirtäjä. Tiedonsiirtäjällä tarkoitettaisiin sellaista tahoa, joka omistaa tai hallinnoi viestintäverkon sitä osaa, joka ylittää Suomen rajan. Siviilitiedustelulaissa ei velvoitettaisi muita yksityisiä kuin tiedonsiirtäjiä. Lisäksi on huomioitava, että laissa ei säädettäisi velvollisuudesta luovuttaa salausavaimia suojelupoliisille tai asentaa niin sanottuja takaportteja ohjelmistoihin tai laitteisiin. Näitä velvoitteita ei myöskään olisi sotilastiedustelulain puolella. (Sisäministeriön julkaisu 8/2017, 150.)

Tiedonsiirtäjän velvollisuuksina olisi myötävaikuttaa tietoliikennetiedustelun edellyttämän liityntäpinnan rakentamista omistamassaan tai hallitsemassaan tietoverkossa, joka ylittää Suomen rajan. Lisäksi tiedonsiirtäjän tulisi luovuttaa suojelupoliisille sellaiset tiedot viestintäverkosta, mitkä olisivat välttämättömiä tuomioistuimelle esitettävää lupavaatimusta varten. Laissa määritellyllä tiedonsiirtäjällä olisi lain mukaan oikeus saada korvaus sille aiheutuneista välittömistä kustannuksista ja suojelupoliisi päättäisi oikeudesta näihin korvauksiin. (Sisäministeriön julkaisu 8/2017, 151.)

Hallituksen esityksen (HE 202/2017 vp) maininnan mukaan Euroopan ihmisoikeustuomioistuin on katsonut, että luottamuksellisen viestin suojaan puuttuvista tiedonhankintakeinoista tulee päättää tuomioistuin. Lisäksi kansallisen lain on sisällettävä riittävät kriteerit, jotka ohjaavat tuomioistuimen lupaharkintaa. Lakiehdotuksen mukaan tietoliikennetiedustelua koskevat lupa-asiat käsiteltäisiin sekä ratkaistaisiin Helsingin käräjäoikeudessa osaksi siitä syystä, että kyseisellä käräjäoikeudella on maan laajin kokemus salaisten tiedonhankinta- ja pakkokeinoasioiden käsittelemisestä. Tietoliikennetiedusteluun liittyvästä suojelupoliisin lupavaatimuksesta sekä tuomioistuimen myöntämästä lupapäätöksestä tulee käydä ilmi tiedustelun kohteena oleva kohde ja ne tosiseikat, joihin tiedustelumenetelmän käyttö perustuu (esimerkiksi vakava uhka kansalliselle turvallisuudelle). Lisäksi tulisi tehdä selkoa lukuisista muista asioista, kuten käytettävistä hakuehdoista, rajan ylittävän viestintäverkon osasta sekä luvan tarkasta voimassaoloajasta. Tietoliikennetiedustelua voitaisiin myöntää enimmillään lupa kuudeksi kuukaudeksi kerrallaan.

Tämän työn seuraavassa luvussa pyritään kuvaamaan millainen suhde mahdollisella siviilitiedustelulailla olisi yritystoimintaan sekä millaisia vaikutuksia säädettävällä lakikokonaisuudella voisi olla niin elinkeinoelämän kuin kansantalouden näkökulmista.

6 Siviilitiedustelulainsäädännön suhde yritysten toimintaan

Suomessa yksityisen ja julkisen sektorin raja on varsinkin tietyillä aloilla hyvin häilyvä. Nykyisellään yhteiskunnan kriittisiin toimintoihin kuuluvat esimerkiksi seuraavat kokonaisuudet: energia- ja vesihuolto, rahoitusala, viestintä- ja tietotekniikka, elintarvikehuolto, logistiikka sekä terveydenhuolto. Yksityinen sektori tuottaa merkittävän osan julkisista palveluista sekä mahdollistaa yhteiskunnan kriittisen infrastruktuurin toimivuuden kannalta tarpeellisten toimintojen olemassaolon. Lisäksi elinkeinoelämällä on merkittävä rooli kansantalouden näkökulmasta.

Siviilitiedustelulakityöryhmän mietinnön mukaan Suomen kansantalouden sekä sen osaksi kuuluvien yritysten toimintaedellytysten näkökulmasta on tärkeää, että maahan luodaan selkeä säädösperusta tiedusteluviranomaisten toiminnalle. Lainsäädännön riittävä täsmällisyys sekä

tasapaino luo ennakoitavuutta yritysten toiminnan suunnittelun ja investointipäätösten kannalta. Tiedustelua koskevan sääntelyn ja tietosuojan merkityksen korostuessa digitalisoituvilla markkinoilla voi täsmällisellä, tasapuolisella sekä oikeasuhtaisella sääntelyllä olla parhaimmillaan Suomen kansainvälisillä markkinoilla myönteinen kilpailutekijä. (Sisäministeriön julkaisu 8/2017, 165.)

Käynnissä olevan tiedustelulakihankkeen yhtenä päätavoitteena on ollut parantaa Suomen kansallista turvallisuutta, johon elinkeino- ja yrityselämä kuuluvat oleellisena osana. Elinkeinoelämän keskusliitto (EK) on ollut tiiviisti mukana tiedustelulainsäädännön valmistelussa. EK on pyrkinyt korostamaan valmistelutyössä hyvää yrityssalaisuuden suojaa, viranomaisten ja yrityskentän yhteistyötä erilaisten turvallisuusuhkien torjunnassa sekä nopeasti kehittyvän teknologian roolia. EK korostaa kuitenkin, että ettei tulevat uudistukset saa aiheuttaa elinkeinoelämälle kustannuksia tai heikentää yritysten kilpailukykyä tai toimintamahdollisuuksia. Valmisteilla olevan lainsäädännön tulee huomioida elinkeinopoliittiset kysymykset tarkasti, koska kansainvälisessä kilpailussa investoinnit pyrkivät hakeutumaan vakaaseen sekä ennustettavaan ympäristöön. (Elinkeinoelämän keskusliitto 2017.)

Hallituksen esityksen (HE 202/2017 vp) mukaan Suomen elinkeinorakenne on muuttunut entistä palvelukeskeisemmäksi ja talous ylipäätänsä innovaatiolähtöiseksi. Suomessa ollaan siirrytty osaamis- ja teknologiaintensiivisille aloille, mitkä houkuttelevat ulkomaisia sijoittajia. Suomen erityiseksi vahvuudeksi kansainvälisessä kilpailussa on noussut informaatio- ja viestintäteknologia. Tietointensiivisen teollisuuden kansantaloudellinen merkitys on nousussa. Käynnissä olevalla lainsäädäntötyöllä on pyritty arvioimaan tiedustelulakien vaikutusta Suomen kansainväliseen kilpailukykyyn sekä houkuttelevuuteen investointikohteena.

Haastateltu professori näkee tiedustelulakikokonaisuudelle tarpeen myös yritysten kannalta. Hänen mukaansa lainsäädäntö parhaimmillaan lisää suomalaisten yritysten kyberturvallisuutta ja ennen kaikkea sitä havaintokykyä, että tiedetään paremmin mitä yritysten tietoverkoissa tapahtuu. Toki yritykset ovat olleen lainsäädäntötyön aikana huolestuneita muun muassa takaporttien tekemisestä tai salausavaimien luovuttamisesta, mutta näitä kumpaakaan ei ole tulossa esitettyyn lainsäädäntöön. Tällä hetkellä yritykset ovat ehkä hieman epätietoisuuden tilassa, että mitkä tiedustelulainsäädännön vaikutukset tulevat olemaan ja ennen kaikkea millaisia hyötyjä se voi parhaimmillaan tuoda yrityksille.

Lähitulevaisuudessa yritysten tulee muutenkin huomioida oma tietosuojansa ja kyberturvallisuutensa tasonsa. Euroopan unionissa hyväksyttiin yleinen tietosuoja-asetus, jonka soveltaminen alkaa 25.5.2018. Tietosuoja-asetus tai GDPR (General Data Protection Regulation) tulee muuttamaan merkittävästi nykyistä henkilötietojen käsittelyä koskevaa sääntelyä yrityksissä. Voimaantuleva tietosuoja-asetus tuo erilaisia velvoitteita ja se laajentaa merkittävästi ihmis-

ten oikeuksia omiin henkilötietoihinsa nähden. Yritysten on otettava huomioon nämä muuttuneet velvoitteet ja oikeudet asiakkaiden, yhteistyö- ja sidosryhmäkumppaneiden tai työntekijöiden kanssa toimittaessa, erityisesti henkilötietojen hallinnan ja käsittelyn osalta. GDPR:ään liittyvät erilaiset maine-, vahingonkorvaus- ja sanktioriskit, mitkä pakottavat jokaisen henkilötietoja käsittelevän yrityksen huomioimaan uuden sääntelyn ja tarvittaessa mukauttamaan toimintansa tämän mukaiseksi. (Varsinais-Suomen yrittäjät 2017.)

Siviilitiedustelulakikokonaisuudesta todennäköisesti suurimpana elinkeinoelämää ja yrityksiä kiinnostavana osa-alueena on tietoliikennetiedustelu. Yleinen digitalisaatiokehitys on luonut yrityksille moninaisia liiketoimintamahdollisuuksia ja yrityskenttään on syntynyt kokonaan uusia liiketoiminta-alueita, joista esimerkkeinä voidaan mainita pilvipalvelut, globaalit konesalitoiminnot sekä kyberturvallisuuden toimiala. On siis ilmeistä, että tietoverkottumisen ja teknologiakehitys myötä, myös rikollinen toiminta on siirtynyt sähköisempään maailmaan. Tämän vuoksi yritysten tulee huomioida entistä paremmin toimintaedellytyksensä ja toiminnan turvaamisen moninaisen pelikentän myös tulevaisuudessa. Tältä näkökannalta Suomeen luotavalla tietoliikennetiedustelukyvykkyydellä voi olla suuriakin hyötyä niin valtakunnan turvallisuuden kuin yritysmaailmankin kannalta.

6.1 Digitalisaation merkitys elinkeinoelämälle

Yhteiskuntamme on tietoteknistynyt ja digitalisoitunut huimaa vauhtia. Digitalisaation ympärille on syntynyt kokonaan uusia liiketoiminta-alueita ja perinteisetkin alat hyödyntävät digitalisaation mahdollisuuksia entistä tehokkaammin. Tilastokeskuksen teki vuonna 2014 digitalisaation merkitystä yritysten liiketoiminnassa käsittelevän tutkimuksen (Tilastokeskus 2014.), jossa tarkasteltiin vuosina 2012-2014 yritysten näkemyksiä digitalisaatiosta sekä sen hyödyntämisestä liiketoiminnassa. Tutkimuksen tulosten mukaan voidaan arvioida, että digitalisaatio vaikuttaa merkittävästi yritysten toimintaan. Vastanneista yrityksistä 38 prosenttia arvioi, että digitalisaation merkitys markkinoinnissa on joko suurta tai kohtalaista sekä 36 prosenttia piti digitaalisten tuotteiden olevan merkittäviä yrityksen liiketoiminnalle. Noin kolmannes vastanneista arvioi pilvipalveluiden, esineiden internetin ja digitalisaation roolin tuotteiden tuottamisessa ja palveluiden jakelussa merkittäväksi. (Tilastokeskus 2014.)

Digitalisaatio ja tätä kautta kyberturvallisuus luovat toisaalta haasteen yritystoiminnan jatkuvuudelle ja kehittymiselle. Turvallisuuden näkökulmista yritykset harjoittavat edelleen melko perinteistä turvallisuussuunnittelua varsinkin tietojärjestelmien ja tietotekniikan maailmassa. Haastatellun kyberturvallisuusjohtajan mukaan Suomessa ollaan ylioptimistisia oman toimintansa puolustuksen suhteen. Yritykset uskovat edelleen erilaisten teknisten turvallisuusratkaisujen voimaan, vaikka todellisuudessa tulisi keskittyä oman ympäristönsä tilannetietoisuuden parantamiseen ja oikeiden havaintojen sekä niitä seuraavien toimenpiteiden tekemiseen

Käynnissä oleva lainsäädäntöhanke on pyrkinyt huomioimaan monella eri tasolla esimerkiksi siviilitiedustelulakikokonaisuuden ja tietoliikennetiedustelun merkitystä myös elinkeinoelämän näkökulmasta. Hallituksen esitys siviilitiedustelulaista kuvaa globaalin ja digitalisoituneen yritystoiminnan nykytilaa, jossa fyysisillä valtioiden rajoilla ei ole suurta merkitystä toiminnan kannalta. Elinkeinoelämä elää globaalissa, kansainvälisen talouden maailmassa, jossa pienetkin tekijät ovat merkityksellisiä globaalille kilpailulle. Yritykset pyrkivät sijoittamaan toimintonsa maakohtaisesti ja samalla optimoimaan toimintaansa yrityskohtaisten kilpailuetujen perusteella. Investointi- ja sijoittamispäätösten taustalla on vankka harkinta ja kokonaisarvio, mikä perustuu muun muassa markkinatekijöihin, verotukseen, energian saatavuuteen, teknologiseen osaamiseen, työvoiman koulutustasoon, yhteiskunnan ja infrastruktuurin kehittymiseen sekä poliittiseen vakauteen ja ennakoitavuuteen. Investointikohteena Suomi näyttäytyy hyvin luotettavana ja vakaana kohteena, mutta tietyt asiat vaativat lisäsääntelyä, kuten tietoliikenneympäristön valvonta selkeine pelisääntöineen. (HE 202/2017 vp.)

Tällä hetkellä esimerkiksi tietoliikennetiedustelua ei ole säännelty millään tavoin, joten suomalaisilla viranomaisilla ei ole juuri mahdollisuuksia saada näkyvyyttä ja havaintotietoa mitä tietoverkoissa tapahtuu. Huomionarvoista on kuitenkin se, ettei muodostettava tietoliikennetiedustelulaki teknisine toteutuksineen tule olemaan minkäänlainen tietoturvakomponentti, joka syrjäyttäisi yritysten oman turvallisuussuunnittelun sekä käytännön toimien toteuttamisen. Haastatellun professorin mukaan tämä lainsäädäntö voi parhaassa tapauksessa täydentää kokonaisturvallisuutta, jos lainsäädäntö esimerkiksi antaa viranomaisille mahdollisuuden luovuttaa tietoja kyberhyökkäyksen tai yritysvakoilun kohteeksi joutuneelle yritykselle. Tässä mielessä kyseisellä lainsäädännöllä voidaan turvata myös elinkeinoelämän olemassaoloa, joka on merkittävää yhteiskunnan toiminnan kannalta.

6.1.1 Kyberturvallisuuden rooli yrityksille

Limnéll et al. kirjoittavat kyberturvallisuutta käsittelevässä kirjassaan kyberturvallisuuden merkityksestä yrityksille. Heidän mukaan yrityksissä on perinteisesti tietoteknistä turvallisuutta tarkasteltu tietoturvallisuuden näkökulmasta, minkä kohteena on yrityksen tietopääoma. Tietoturvan tavoitteena on ollut turvata tiedon luotettavuus, eheys ja saatavuus ja tämä onkin korostunut verkkoturvallisuuden aikakautena. Kyberturvallisuus on tietoturvaa merkittävästä laajempi ja kokonaisvaltaisempi kokonaisuus, joka tuo turvallisuuden kohteeksi ihmisten ja bittien maailman yhdessä muodostaman kokonaisuuden. Nykyisessä kybermaailmassa tietoturva-ajattelu ei yksinään riitä enää. (Limnéll et al. 2014. 55-56.)

Nykypäivän yritystoiminnassa korostuu tietoverkottuminen niin kansallisesti kuin kansainvälisestikin. Tietoverkot yhdistävät yrityksen eri toimipaikkoja, yhteistyökumppaneita ja muita sidosryhmiä. Merkittävimpiä muutoksia kiihtyvässä tietoverkottumisessa on se, ettei yksikään yritys tai toimija hallitse enää täysin omaa tuotanto- ja viestintäprosessiaan. Yritysten toiminta on riippuvainen toisten toimista ja niin edelleen. Harva yritys kuitenkaan tietää, että millaisista monimutkaisista ketjuista, linkityksistä sekä riippuvuuksista sen toimintakyky riippuu. Esimerkkinä voidaan pitää sitä, että kolmannen osapuolen tietojärjestelmät voivat mahdollistaa pääsyn yrityksen luottamuksellisiinkin tietoihin. Kybermaailman ja sen riippuvuuksien tuntemisen tulisi olla yrityksille ensiarvoisen tärkeätä, sillä usein yrityksen ydintoiminta on bittien ohjaamaa tai mahdollistamaa. Näistä syistä myös kyberturvallisuus tulisi nostaa strategisen tason kysymykseksi yritysten johdossa. (Limnéll et al. 2014. 55.)

Suomen kyberturvallisuusstrategian mukaan Suomi on yhteiskuntana riippuvainen tietoverkkojen ja tietojärjestelmien toiminnasta sekä näin ollen erittäin haavoittuvainen näihin kohdistuville häiriöille. Kybertoimintaympäristöön kohdistuvat uhat ovat muuttuneet seurauksiltaan entistä vaarallisemmiksi yksittäisten kansalaisten, yritysten sekä koko yhteiskunnan kannalta. Uhkia muodostavat tahot ovat erityisen ammattimaisia ja nykyisin niihin voidaan laskea myös valtiolliset toimijat. Kybertoimintaympäristö tulee nähdä myös mahdollisuutena ja voimavarana. Turvallinen kybertoimintaympäristö helpottaa ihmisten ja yritysten oman toiminnan suunnittelua ja täten lisää taloudellista aktiviteettia. Hyvä ja terve ympäristö parantaa myös Suomen kansainvälistä houkuttelevuutta investointikohteena. Kansallinen kyberturvallisuus ja kotimaisten yritysten menestys ovat yhteydessä keskenään. (Turvallisuuskomitea 2013, 1.)

Haastatteluiden yhtenä keskeisenä näkökulmana oli myös selvittää suomalaisten yritysten kyberturvallisuuden tasoa tällä hetkellä. Yritysturvallisuuden asiantuntijan mukaan kansainvälisesti vertailtuna suomalaisten yritysten kyberturvallisuuden taso on kohtalaisella tasolla, mutta suuria vaihteluita on paljon eri toimialojen kesken. Suuret pörssiyritykset ovat huomioineet kyberturvallisuuden hyvin, mutta suuria osa pienistä ja keskisuurista yrityksistä ei ole vielä huomanneet niitä hyötyjä, joita kyberturvallisuus tuo tullessaan. Digitalisaatiokehitys tulee kuitenkin jatkossa korostamaan sitä, että kaikki organisaatiot joutuvat entistä enemmän panostamaan kyberturvallisuuteen, koska peruskommunikaatiosta lähtien yritysten toiminta tulee painottumaan tietoverkkoihin. Asiantuntijan mukaan kyberturvallisuuden pitäisikin olla yrityksille strateginen kysymys. Liiketoimintanäkökulmasta kyberturvallisuuteen liittyvien asioiden huomiointi on oleellinen asia, jotta yritys voi tehdä päätöksentekoa laadukkaasti.

Haastateltu professori näkee yritysten kyberturvallisuuden tasossa kehitettävää. Hänen mukaan tutkimukset osoittavat, että Suomi ei ole kyberturvallisuuden kärkimaa, vaikka sitä on tavoiteltu kansallisessa kyberturvallisuusstrategiassa. Kokonaisuutena katsoen Suomi kuuluu kuitenkin globaaliin kärkikymmenikköön, mutta haastetta lisää kyberturvallisuuden muodos-

tuminen monista asioista. Suomen kannalta ihmisten osaamistaso on korkealla tasolla, mutta Suomen sijoitusta laskee kyberturvallisuuteen liittyvän lainsäädännön puuttuminen. Yritysten kyberturvallisuuden näkökulmasta suuret pörssiyritykset ovat varautuneet ja tiedostaneet kyberturvallisuuden tärkeyden ja osaltaan näkee siinä myös uusia liiketoimintamahdollisuuksiakin.

6.1.2 Liiketoiminnan tietopääoma ja sen suojaaminen

Miltei kaikessa yritysten liiketoiminnassa on jotain luottamuksellista tietoa, mitä yritys haluaa pitää salassa erityisesti muilta kilpailijoilta. Tällaiselle tiedolle on ominaista se, että tiedon paljastuminen aiheuttaisi todennäköisesti merkittävää vahinkoa, joten tiedon omistaja haluaa pitää tiedon salassa. Yrityksille tiedon merkitys on useimmiten juuri sen salassa pitämisellä saavutettava kaupallinen arvo eli käytännössä kilpailuetu. Tällaista tietoa kutsutaan yrityssalaisuudeksi, liikesalaisuudeksi tai ammattisalaisuudeksi. Tieto voi hyvin olla joko teknistä (tuotteen valmistusmenetelmä tai kaava) tai sitten taloudellista (liikesopimus, asiakastiedot tai budjetti). (Vapaavuori 2016, 15.)

Nykyisen digitalisaation ja tietoyhteiskunnan kehityksen myötä tiedon ja erityisesti luottamuksellisen tiedon määrä ja merkitys on kasvanut. Aikaisemmin yrityksen merkittävintä pääomaa olivat erilaiset koneet, tuotantotilat tai laitteet, niin nykyisellään yrityksen henkinen pääoma on tärkeintä. Useimmiten yritysten huomattavin varallisuus onkin aineettomissa oikeuksissa, kuten patenteissa, tavaramerkeissä ja yrityssalaisuuksissa. Tilanne muuttuu hieman monimutkaiseksi verkostoituneessa yhteiskunnassa, missä on entistä yleisempää se, että yritys ei itse suunnittele, valmista tai myy tuotteitaan tai palveluitaan, vaan osa näistä toiminnoista tehdään eri yhteistyö- tai alihankkijakumppaneiden välityksellä. (Vapaavuori 2016, 15-16.) Tiedon merkitys yritystoiminnassa on kasvussa erityisesti Suomen kaltaisissa yhteiskunnissa, jossa elinkeinorakenne on muuttunut entistä palvelukeskeisemmäksi sekä talous innovaatiolähtöiseksi. Suomi on siirtynyt osaamis- ja teknologiaintensiivisille aloille, jotka houkuttelevat ulkomaisia sijoituksia maahan. Kansainvälisessä vertailussa Suomen vahvuusalaksi on noussut informaatio- ja viestintäteknologia. Tietointensiivisen teollisuuden taloudellinen merkitys on nousussa ja sen vaikutukset yritystoiminnalle ovat erilaiset riippuen yrityksen toimialasta, koosta sekä sen harjoittamasta kansainvälisestä toiminnasta. (Sisäministeriön julkaisu 8/2017, 166.)

Keskuskauppakamarin vuonna 2017 julkaiseman ”Yritysten rikosturvallisuus 2017” tutkimuksen mukaan 43 prosenttia vastanneista yrityksistä tunnistaa, että niillä on tietoa tai muuta omaisuutta, mikä saattaa olla laittoman tiedustelun kohteena. Suuri osa yrityksistä ei osaa sanoa, mitä tietoja mahdollinen tunkeutuja tai vaikka yrityksen työntekijä voisi viedä ulos yrityksestä. Liiketoiminnan kannalta kriittistä tietoa ei siis välttämättä tunnisteta yrityksissä täysin.

Yritystiedon luvattomasta urkinnasta tai yritysvakoilusta ilmoitti lähes kymmenesosa yrityksistä. Teollisuuden yrityksillä noin puolella on oman kertoman mukaansa sellaista tietoa, joka saattaisi olla laittoman tiedustelun tai yritysvakoilun kohteena. (Keskuskauppakamari 2017, 24.)

Yritykselle elintärkeän tiedon suojaaminen vaatii uusia toimintatapoja, sillä erityisesti kyberuhkat ovat tuoneet uusia haasteita muun muassa tietovuotojen hallinnan suhteen. Perinteisesti oikeusajattelumme on rakentunut sille ideologialle, että oikeussäännökset soveltuvat hyvin paperisidonnaisiin järjestelyihin, suullisen ja kirjallisen esityksen kahtiajakoon. Entistä nopeampi teknologian kehittyminen on kuitenkin saanut aikaan lainsäädännön tasolla uudenlaisen haavoittuvuuden alueen, johon sisältyvät lähestulkoon jokaisen yritystoimintaa harjoittavan yhteisön tai yrityksen tärkeimmät resurssit, aineettomat tiedot. Tietotekniikan käytön lisääntyminen ja kybertoimintaympäristön hyödyntäminen yritystoiminnassa ovat kasvattaneet mahdollisuuksia hankkia suojattua tietoa laittomasti muun muassa tietoverkkojen avulla tai niiden välityksellä. (Oittinen 2016, 41.)

Valtioneuvoston julkaiseman Suomen kyberturvallisuuden nykytilaa, tavoitteita ja tarvittavia toimenpiteitä tavoitetilan saavuttamiseksi tehdyn tutkimuksen mukaan Yhdysvaltojen suurin teleoperaattori AT&T on maininnut, että pelkästään USA:n hallitus kertoo kybervakoilun olevan merkittävin ja yhä kasvava uhka valtion turvallisuudelle sekä sen menestykselle. Erilaiset kybervakoiluryhmät ovat kiinnostuneita aineettomasta omaisuudesta, liikesalaisuuksista, kansallisista salaisuuksista, sotilaallisesta luottamuksellisesta tiedosta sekä valtiontasoisiin prosesseihin vaikuttamisesta. Kybervakoilua tekevät valtiot ja yritykset unohtamatta järjestäytynyttä rikollisuutta. Näiden toimijoiden suorittama kybervakoilu jatkaa kasvuaan ja muuttuu yhä monimuotoisemmaksi. Usein kybervakoilun takaa löytyykin valtion tukemia ryhmittymiä ja raja valtiollisen ja teollisen vakoilun välillä alkaa olla häilyvä. Rajan epämääräisyys näkyy erityisesti niissä tapauksissa, joissa suuret monikansalliset toimijat ovat mukana, tai kampanjoissa, joissa kansallisten toimijoiden lisäksi mukana on aggressiivisia aktivistiryhmiä, kilpailijoita sekä teollisuusvakoilua. (Valtioneuvoston kanslia 2017, 20-21.)

Opinnäytetyöhön haastateltiin muun muassa eri suomalaisia kyberturvallisuuden palveluita tarjoavien yritysten asiantuntijoita. Haastatellun tietoturvajohtajan mukaan julkisuudesta saatava kuva suomalaisten yritysten kyberturvallisuuden ja tiedon suojaamisen tasosta on osin virheellinen. Hänen käytännön kokemuksensa mukaan muun muassa isojenkin suomalaisten yritysten tuotekehitysympäristöissä on ollut nähtävissä merkittäviä ongelmia. Hän lisää vielä, että suomalaiset tietoverkot saattavat olla melko puhtaita, mutta yritysten tai kriittisen infrastruktuurin järjestelmiä ei ole suojattu ainakaan merkittävästi paremmin kuin muuallakaan maailmassa.

Suomalaisen kyberturvallisuuspalveluita tarjoavan yrityksen asiantuntijoiden mukaan yritysten tiedon suojaaminen on hyvin pitkälle ollut estämiskeskeistä, jossa on keskitytty yrityksen ulkokuoren koventamiseen teknisillä järjestelmillä, mutta itse havainnointipuoli on puuttunut. Heidän tutkimissaan tietomurtotapauksissa usein havainnointikyvyn puuttuminen on aiheuttanut sen, että järjestelmiin tai verkkoihin hyökännyt on voinut olla yrityksen sisällä jopa vuosia, kunnes ulkopuolisilta tahoilta on tullut yritykselle tullut vinkki, että yrityksen IP-osoitteesta tulee epäilyttävää liikennettä. Puolustusmielessä vanhat mallit eivät riitä pelkästään, vaan yrityksiltä vaaditaan ajattelutavan muutosta siinä mielessä, että hyökkääjä löytää aina tavan päästä yrityksen järjestelmiin käsiksi. Tästä syystä tulisikin entistä enemmän panostaa tilannetiedon oikeellisuuteen ja reagoida tarkoituksenmukaisesti havaittuihin puutteisiin tai rikkomuksiin.

6.1.3 Viranomaisten sekä yritysten toimenpiteet kyberuhkien torjunnassa

Limnéll et al. kirjoittavat Kyberturvallisuus-teoksessa, että ollakseen menestyvä, uskottava ja luotettava toimija nykyisessä kansainvälisessä turvallisuuspolitiikassa sekä kilpailukykyinen globaalissa taloudessa, on itsenäisellä valtiolla oltava myös kyberturvallisuusasiat kunnossa. Valtion merkitys yhteiskunnan kyberturvallisuuden tuottamisessa on moninainen. Ensimmäiseksi valtion sääntelee ja ohjeistaa yhteiskunnan toimintaa sellaisella tavalla, että sillä pystytään tuottamaan paras mahdollinen turvallisuus. Toiseksi valtio pyrkii turvamaan omat kyberalttiit prosessinsa. Kolmanneksi valtion tulee tiedottaa kyberturvallisuuteen liittyvistä asioista sekä järjestää rakenteet ja toimintatavat siten, että ne auttavat yhteiskunnan kannalta vakavien turvallisuusloukkausten kohteeksi joutuneita. Neljänneksi valtio ohjaa ja järjestää yhteistyössä yksityisen sektorin kanssa yhteiskunnan varautumista erilaisiin häiriötilanteisiin ja poikkeusoloihin etenkin kriittisen infrastruktuurin osalta. Viidentenä valtion tulee osaltaan varmistaa, että yhteiskunnan toimijoita opetetaan ja koulutetaan aina yksilöön asti toimimaan vastuullisesti kybertoimintaympäristöissä. Lopuksi valtio reagoi ja vastaa yhteiskuntaan kohdistuneisiin vakaviin kyberhyökkäyksiin ja siihen kohdistuviin kyberuhkiin tarpeelliseksi katsotulla tavalla. (Limnéll et al. 2014, 58-59.)

Siviilitiedustelulakikokonaisuutta käsittelevät hallituksen esityksen (HE 202/2017 vp) mukaan turvallisuusviranomaisten arvion mukaan useat ulkomaiset valtiot pyrkivät toiminnassaan kohdistamaan laajaa sekä teknisesti kehittynyttä kybervakoilua Suomen valtionhallintoon ja kansantaloudellista merkitystä omaaviin yrityksiin. Kyberympäristössä tapahtuvassa vakoilussa käytettävinä tekovälineinä ei ole tavallisia kaupallisilla virustorjuntaohjelmistoilla havaittavia haittaohjelmia, vaan teknisesti kehittyneitä sekä monipuolisia tietoverkkohyökkäystyökaluja. Hyvin usein vakoiluoperaatio on tarkasti suunniteltu ennakkoon ja sillä on täsmällinen tavoite kerätä tietoa esimerkiksi ulko- ja turvallisuuspolitiikkaan tai talouteen sekä teollisuuteen liittyvistä asioista. Yhtenä esimerkkinä tällaisista vakoiluoperaatioista voidaan pitää ulkoministe-

riöön kohdistettu tapaus, joka tuli ilmi vuonna 2013. Hyökkäyksissä käytettyjen tiedusteluohjelmien lisäksi tietojärjestelmiin voidaan toimittaa haittaohjelmia, jotka aktivoituvat kriisin alkaessa.

Valtioneuvoston kanslian vuonna 2017 julkaiseman riippumattoman tutkimuksen mukaan Suomen kansallinen kyberturvallisuuteen liittyvien tapahtumien havainnointikyky on puutteellinen. Tämän vuoksi tilannetietoisuus on heikko ja edellytykset estää, rajoittaa ja toipua vakavista kyberhyökkäyksistä on tällä hetkellä rajallista. Tutkimus valottaa, että suomalaisen yhteiskunnan kaikkia elintärkeitä toimintoja sekä huoltovarmuuskriittisiä yrityksiä ei ole tällä hetkellä suojattu riittävän korkealla tasolla erilaisia kyberuhkia vastaan. Lisäksi häiriötilanteiden sietokyky (resilienssi) on edelleen osassa suojattavia kohteita heikolla tasolla. Suomen lainsäädäntöä ei ole kyetty nykyaikaistamaan kyberturvallisuuden vaatimuksia vastaaviksi. Käynnissä olevan tiedustelulainsäädännön uudistaminen arvioidaan tutkimuksessa välttämättömäksi havainnointikyvyn parantamiseksi. (Valtioneuvoston kanslia 2017, 69.)

Yllä mainitut haasteet aiheuttavat yhteiskunnallisesti tarkasteltuna merkittäviä haasteita liittyen kyberuhkien torjuntaan. Suomen kokoisen maan tapauksessa viranomaisten ja yritysten yhteistyö korostuukin. Kansallisen kyberturvallisuusstrategian mukaan kyberturvallisuuden järjestelyissä noudatetaan viranomaisten, yritysten ja järjestöjen välillä vastuunjakoa, joka perustuu säädöksiin ja sovittuun yhteistyöhön. Strategiassa tehtyjen linjausten toimeenpanolla pyrittiin vahvistamaan julkisen ja yksityisen sektorin välistä yhteistoimintaa. Tämän yhteistyön avulla voitaisiin parhaiten palvella koko yhteiskuntaa ja tukea sen elintärkeitä toimintoja tuottavia toimijoita. (Turvallisuuskomitea 2013, 5-6.)

Suomessa Viestintäviraston alaisuudessa toimiva Kyberturvallisuuskeskus toimii kansallisena yhteydenottopisteenä tietoturvaloukkauksien vastaanottamiseksi. Lisäksi keskus varoittaa yhteiskunnan elintärkeiden toimijoiden kannalta tärkeitä yrityksiä ja viranomaisia Suomea uhkaavista tietoturvapoikkeamista ja -uhista sekä tarvittaessa avustaa näihin varautumisessa. Kyberturvallisuuskeskus tuottaa myös erilaisia tilannekuvapalveluita, joiden käyttäjinä toimivat suomalaiset teleyritykset, ICT-toimijat, finanssialan yritykset, huoltovarmuuskriittiset toimijat mukaan lukien sähköyhtiöt sekä julkishallinto yleisesti. Keskusrikospoliisin kyberkeskus puolestaan vastaa kyberrikoksien tutkinnasta ja toimii kyberrikostorjunnan kansallisen ja kansainvälisen yhteistyön koordinaatiopisteenä. (Viestintävirasto 2014, 1.)

Viestintävirasto on yhteistyössä Huoltovarmuuskeskuksen kanssa luonut erityisesti Suomen huoltovarmuuden kannalta kriittisille yrityksille ja valtionhallinnon toimijoille tietoturvaloukkausten havainnointi- ja varoitusjärjestelmän (HAVARO). Järjestelmän avulla yrityksen tai organisaation verkkoliikenteestä havainnoidaan haitalliseksi tunnistettua tai normaalista poikkeavaa liikennettä. Järjestelmän toiminta perustuu eri tietolähteistä saataviin uhkia koskeviin

tunnisteisiin, joiden avulla organisaation tietoliikenteestä tunnistetaan poikkeavuudet ja muut uhkat. Viestintävirasto vastaanottaa tiedot ja suorittaa niiden analysoinnin. Mikäli analyysin perusteella ilmenee tietoturvauhka, niin siitä varoitetaan yritystä. Vaikka järjestelmä on kehitetty huoltovarmuuskriittisille toimijoilla, niin järjestelmä auttaa yksittäisten organisaatioiden lisäksi muodostamaan kokonaiskuvaa suomalaisiin tietoverkkoihin kohdistuvista kyberturvallisuusuhkista. (Viestintävirasto 2016.)

Haastatellun kyberturvallisuusjohtajan mukaan viranomaisten tuottamien palveluiden lisäksi eri tietoturva- ja kyberturvallisuuspalveluita tarjoavat yritykset sekä muut toimijat tarjoavat kaupallisia kyberuhkien torjuntaan keskittyneitä palveluita, joita erityisesti suurimmat yritykset käyttävät ympäristönsä tilannetiedon parantamiseen. Suomalaisen asiantuntijayrityksen tietoturvajohtajan mukaan yhteistyö on tällä alueella tarpeellista, mutta lähtökohtaisesti yritysten tulisi itse suojata ja tietonsa. Viranomaisten ja yksityisen sektorin yhteistyö parhaimmillaan voi auttaa isompien uhkien, erilaisten trendien havaitsemisen tai kohdistetun tiedustelutoiminnan löytämisen suhteen, mutta ensisijainen vastuu on kullakin toimijalla.

Helsingin seudun kauppakamarin vuonna 2015 tekemä selvitys, johon osallistui 750 suomalaista yritystä, toi esiin huolestuttavia piirteitä kyberturvallisuuteen liittyvän viranomaistoiminnan ja siihen liittyvän yhteistyön tuntemuksesta. Selvityksen mukaan miltei 80 prosenttia yrityksistä ei tiennyt mikä muun muassa on viranomaisten rooli kyberturvallisuuden alueella. Yritysten ja viranomaisten välisen yhteistyön kehittäminen tulisikin selvityksen mukaan ottaa vakavasti, kun halutaan parantaa suomalaisten yritysten kyberturvallisuutta. (Helsingin seudun kauppakamari 2015, 31.)

Käynnissä olevan siviilitiedustelulakihankkeen valmistelussa on pyritty huomioimaan yritysten tarpeet erityisesti tietojen luovutuksen kannalta. Sisäministeriön työryhmän mietinnön (Sisäministeriön julkaisu 8/2017) mukaan tiedustelullisin menetelmin hankittua tietoa voitaisiin tarkoin ja tiukoin edellytyksin luovuttaa esitutkinta- tai muulle toimivaltaiselle viranomaiselle. Hallituksen esityksessä (HE 202/2017 vp) poliisilain 5a luvun 55 pykälä mainitsee, että suojelupoliisilla voi toimia siviilitiedustelutehtävissä yhteistyössä yhteisöjen kanssa ja luovuttaa muille viranomaisille ja yhteisöille tietoja, mikäli niiden luovuttaminen olisi välttämätöntä kansallisen turvallisuuden suojaamiseksi. Yhteistyön merkitys tulee kasvamaan myös tulevaisuudessa ja voimaantullessaan lainsäädäntö tulee käytännössä osoittamaan, että onko laissa mainitunkaltainen tietojen luovutus mahdollista.

6.2 Tietoliikennetiedustelun vaikutukset liiketoimintaan

Tiedustelulainsäädännön valmistelutyössä on pyritty huomioimaan sen mahdollisia vaikutuksia elinkeinoelämälle, ulkomaisille investoinneille sekä Suomen kilpailukyvylle. Tietoliikenne-

tiedustelun kautta saatavilla tiedoilla on ensisijaisesti tarkoitus parantaa Suomen kansallista turvallisuutta. Yhteiskunnan kokonaisturvallisuuden näkökulmasta on ilmeistä, että kyseisillä tiedoilla voi olla myös merkittäviä hyötyjä Suomen taloudellisten intressien näkökulmasta.

Siviilitiedustelulaki valmistelleen sisäministeriön työryhmän mukaan tiedustelulainsäädännön vaikutuksia kansantalouteen, yrityksiin ja elinkeinoelämään tulee arvioida kokonaisuutena. Lainsäädännön seurauksia arvioitaessa tulee ottaa huomioon erityisesti vaikutukset yhteiskunnan digitalisoitumiskehitykseen sekä yritysten toimintaedellytyksiin, sillä talouskasvun kannalta Suomen on välttämätöntä käyttää hyväksi tieto- ja viestintäteknologian myötä tulevat mahdollisuudet toimintatapojen muuttamiseen sekä tuottavuuden parantamiseen. (Sisäministeriön julkaisi 8/2017, 165.)

Samaisen ryhmän mietinnön mukaan olennaista suomalaisten ICT-alan yritysten kilpailukyvyn kannalta on, että ehdotettava sääntely ei velvoita yrityksiä heikentämään tuotteidensa tai palveluidensa luotettavuutta esimerkiksi salausavaimien luovuttamisen, takaporttien asentamisen, salaustuotteiden käyttöön liittyvien rajoitteiden tai muiden liiketoiminnalle haitallisten velvoitteiden seurauksena. Kaikkien Suomessa toimivien yritysten näkökulmasta on pyritty huomioimaan, että tulevasta sääntelystä aiheutuvat velvoitteet olisivat selkeitä, läpinäkyviä sekä ennakoitavissa. Tietoliikennetiedusteluun liittyvällä säännöstelyllä ei tulla siirtämään tiedonsiirtäjinä pidettäville yrityksille tai muillekaan yrityksille sellaisia velvoitteita, jotka kuuluvat yksinomaan viranomaisille. (Sisäministeriön julkaisu 8/2017, 166.)

Puolustusministeriön tiedonhankintalakityöryhmän mietinnön valmistelussa luottamuksellisesti kuullut ulkomaiset asiantuntijat ovat korostaneet, että tietoliikennetiedustelu on keino saada kansalliseen turvallisuuteen kohdistuvien uhkien havaitsemiseksi ja torjumiseksi välttämätöntä tietoa sekä hankkia strategisen tason tietoa valtion ylimmän päätöksenteon pohjaksi. Kuulemisissa tuotiin esille, että tietoliikennetiedustelu myös täydentäisi merkittävällä tavalla Suomen suojautumista vakavimpia tietoverkkouhkia vastaan. Nykyiset järjestelmät eivät todennäköisesti havaitse valtiollisia vakoilu- ja muita haittaohjelmia, joita käytetään tiedustelun toteuttamisessa ja joilla on erityisen suuri kansallista turvallisuutta vahingoittava vaikutus. Tietoliikennetiedustelusta olisi näin ollen hyötyä myös elinkeinoelämän suojautumisessa kaikkein vakavimpia tietoverkkouhkia vastaan. (Puolustusministeriö 2015b, 69.)

Valmistelutyössä on pyritty huomioimaan elinkeinoelämän tarpeita muun muassa pyytämällä monipuolisesti lausuntoja, järjestämällä kuulemistilaisuuksia yrityksille ja ottamaan elinkeinoelämän edustajia osaksi lainsäädännön työryhmiä. Lisäksi elinkeinoelämän oma aktiivinen ote asiassa on edesauttanut yhteistyötä. Elinkeinoelämän keskusliiton tiivistä mukanaoloa sotilas- ja siviilitiedustelulainsäädännön valmistelutyöryhmissä tuki elinkeinoelämän oma seurantaryhmä. EK:n mielestä onkin tärkeätä, että tiedustelu saadaan Suomessa sääntelyn piiriin

ja sen elinkeinopoliittiset kysymykset huomioidaan tarkasti, sillä kansainvälisessä kilpailussa investoinnit hakeutuvat vakaaseen ja ennustettavaan ympäristöön. (Elinkeinoelämän keskusliitto 2017.)

6.2.1 Kyberturvallisuuden tilannekuva yritysten kannalta

Kyberturvallisuuteen liittyvä tilannekuva on yritysten toiminnan kannalta hyvin tärkeää, koska tarkka tilannekuva mahdollistaa oikeiden johtopäätösten tekemisen ja lopulta parantaa toiminnan johtamiseen liittyvää päätöksentekoa yleisesti. Aalto-yliopiston kyberturvallisuuden professori Jarno Limnéll korostaa johtamisen roolia kattavan kyberturvallisuuden tilannekuvan luomisessa. Organisaation johdon määrittelemät arvot ja strategia luovat lähtötilan muun muassa kyberturvallisuuden kaipaamalle sitoutumiselle. (Limnéll 2014.)

Haastatellun kansainvälisen teknologiakonsernin turvallisuusjohtajan mukaan yritysten tilannekuvan ylläpitäminen ja ymmärtäminen on tärkeätä. Hänen mukaansa käynnissä olevalla tietoliikennetiedustelulakihankkeella on selkeitä hyötyjä yritysten kannalta, joista yksi on tietoverkoissa tapahtuvan lisänäkyvyyden saaminen. Yrityksillä saattaa olla käytössä tiettyjä kyberturvallisuuden sekä oman ympäristönsä tilannekuvan havainnointiin luotuja ratkaisuja, mutta harvalla suurellakaan yrityksellä on resursseja tuottaa kattavaa tietoa yksin. Tässä mielessä lainsäädännön tulisi mahdollistaa tehokas yhteistyö viranomaisten kanssa, mutta hänen mukaansa yritys ei voi laskea mitään sen varaan, että viranomainen hoitaisi yrityksen tilannekuvan päivitystä. Yritysten tietoliikennetiedustelun kautta mahdollisesti saama tieto tulisi nähdä vain yhtenä työkaluna muiden joukossa.

Kattavan tilannekuvan ylläpitäminen vaatiikin yrityksiltä verkostoitumista ja yhteistyötä muiden alueen toimijoiden kanssa. Tiedonvaihdon merkityksellä voi olla suuriakin hyötyjä, varsinkin nykyisessä tieverkottuneessa yhteiskunnassa, jossa kyberuhkien leviäminen saattaa tapahtua hyvinkin lyhyen aikana. Yritysturvallisuuden asiantuntijana haastatellun henkilön mielestä kansallisessa mielessä parempi kyberturvallisuuden tilannekuva palvelee laajasti koko yhteiskuntaa, myös yrityksiä.

Asiantuntijan mukaan olisi erityisen tärkeätä huomioida, ettei viranomaiset vaan lainsäädännön turvin kerää tietoa, vaan tätä tietoa tulisi käyttää koko yhteiskunnan hyväksi huomioiden toki toiminnan lainalaisuudet. Hänen mukaansa yritysten liiketoiminnan näkökulmasta tietoliikennetiedustelun kaltaisella lainsäädännöllä tulisikin tavoitella sitä, että Suomen kokonaisvaltainen toimintaympäristö tulee paremmaksi ja turvalliseksi. Mikäli viranomaiset havaitsisivat tiedustelutoiminnassaan, että jokin suomalainen yritys kokee merkittäviä taloudellisia vahinkoja, yritysvakoilua tai muuta vahingollista toimintaa, niin lainsäädännössä tulisi olla

sellainen mekanismi säädeltynä, että yrityksiä voisi tiedottaa asiasta. Toki sitä ei voida varmistaa lainsäädännöllä täysin, että millaisiin toimiin yritys tämän jälkeen ryhtyisi.

6.2.2 Tiedustelulainsäädännön suhde investointeihin

Käynnissä olevan tiedustelulakihankkeen vastustajat ovat käyttäneet yhtenä argumenttinaan sitä, että esimerkiksi tietoliikennetiedustelun mahdollistaminen vähentäisi ulkomaisten yritysten tekemiä investointeja Suomeen. Ruotsissa vuonna 2009 säädetyn vastaavanlaisen signaalitiedustelulain (FRA-laki) pelättiin tuolloin karkottavan maasta ulkomaiset sijoittajat. Viime aikoina on ollut nähtävissä, että tuo pelko ei ole ainakaan Ruotsin kohdalla toteutunut. Muun muassa Facebook on avannut Ruotsiin jo kaksi uutta datakeskusta, joista vuonna 2012 avattu keskus oli aikanaan ensimmäinen Yhdysvaltojen ulkopuolella (Data Center Dynamics 2014). Lisäksi Amazon suunnittelee avaavansa uuden datakeskuksen Tukholmaan pilvipalveluiden tueksi (Fortune 2017).

Lainsäädäntötyötä edeltäneen tiedonhankintalakityöryhmän mietinnön yhteydessä selvitettiin tietoliikenteeseen kohdistuvat tiedustelun mahdollisia negatiivisia vaikutuksia Suomeen kohdistuviin ulkomaisiin investointeihin. Yleisesti selvityksessä havaittiin, että vaikutuksia investointeihin on vaikeata arvioida, mutta vertailukohteena käytettiin yksityiskohtaisesti tietoliikennetiedustelusta säätänyttä Ruotsia. Kyseisessä Ruotsin tapauksessa ei ole nähtävissä sellaista poikkeamaa ulkomaisten investointien kohdalla, jota voitaisiin selittää Ruotsin tietoliikennetiedustelua koskevan lainsäädännön vaikutuksella. Kansainvälisessä Data Center Risk Index -vertailussa Ruotsi on itse asiassa menestynyt Suomea paremmin. (Sisäministeriön julkaisu 8/2017, 166.)

Tiedonhankintalakityöryhmän teettämän selvityksen mukaan Ruotsissa FRA-lain valmisteluvaiheen voimakkaat kannanotot ja toimenpiteet elinkeinoelämän taholta ovat pääosin hiljentyneet. Nykyisellään uutisointi liittyy enemmän kansalaisoikeuksiin, Yhdysvaltain NSA-paljastuksiin sekä poliittiseen keskusteluun asian ja signaalitiedustelun yleisen toiminnan ympärillä. Selvityksen mukaan selkeää yhteyttä FRA-lain mahdollisista vaikutuksista IT-sektorin ulkomaisiin investointeihin kyseisen lain voimaantulon jälkeen tai eroavaisuuksia samantyyppisiin investointeihin Suomessa ei todettu. Toisaalta selvityksessä ilmeni, että täsmällisesti säädetty lakikokonaisuus luo ennustettavamman toimintaympäristön kaikille ICT-sektorin toimijoille ja näin ollen myös investoinnit ovat luotettavammalla pohjalla. (Puolustusministeriö 2015b, 95.)

Hallituksen esityksessä (HE 202/2017 vp) on mainittu myös, että luotava tiedustelujärjestelmä tulee Suomessa vaatimaan viranomaisten investointeja osaamiseen ja käytettävään teknologiaan. Säädettävänä olevat tiedonhankintatoimivaltuudet edellyttävät erilaisia teknologisia in-

vestointeja ja yleistä panostamista turvalliseen tuotekehitykseen. Tiedustelutoiminta on luonteeltaan sellaista, että investoinneissa on huomioitava erityisesti käytettävän teknologian turvallisuus sekä toiminnan kannalta erilaiset huoltovarmuuskysymykset. Samalla viranomaisen omat resurssit ovat rajalliset ja tästä syystä tulee huomioida mahdollisuudet sopimusperusteisen palvelutuotannon hyödyntämiseen yksityiseltä sektorilta. Tämä voi tarkoittaa nopeasti kehittyvän digitalisaation aikakautena uusien liiketoimintamallien, työpaikkojen sekä osaamisen syntymistä Suomeen.

Tutkimuksen haastattelujen kautta oli havaittavissa, ettei asiantuntijatkaan koe käynnissä olevaa lainsäädäntöhanketta uhkana investoinneille. Elinkeinoelämän näkökulmasta haastatellun yritysturvallisuusasiantuntijan mukaan nyt luotavan lainsäädännön tulee olla avoin ja selkeä, joka olisi myös kaikkien Suomeen investointeja harkitsevien organisaatioiden käytössä. Hänen mukaansa on vaikeata nähdä, että Suomeen suunniteltu lainsäädäntö poikkeaisi ainakaan negatiivisesti mistään Euroopassa jo olevasta lainsäädännöstä. Tarkalla lainsäädännöllä ennemmin poistetaan epävarmuuksia investoinneilta kuin aiheutetaan niitä.

Suomalaisen yliopiston professori oli samoilla linjoilla liittyen tiedustelulainsäädännön vaikutuksiin investointihalukkuudessa. Professorin mukaan parhaimmillaan lainsäädäntö lisää suomalaisten yritysten kyberturvallisuutta ja ennen kaikkea tietoverkoissa tapahtuvaa havainnointikykyä. Investointimielessä tärkeätä on saada Suomelle sellaiset tiedustelulait, joiden kautta syntyy selkeät pelisäännöt ja tehokas valvonta. Suurien kansainvälisten datakeskuspalveluita tarjoavien yritysten kannalta on investointipäätökset kohdistuvat sellaisiin maihin, joissa on määritelty tarkasti miten tiedustelutoimintaan harjoitetaan. Lisäksi on muistettava, että useat maat Euroopassa kuin muuallakin suorittavat samanlaista tiedustelutoimintaa, joten kansainväliset yritykset ovat jo huomioineet tämän toiminnassaan.

Yritysturvallisuuden asiantuntija muistuttaa, että parhaimmillaan tiedustelulainsäädännön ympärille voi lähteä kasvamaan kokonaan uusia yrityksiä sekä innovaatioita. Tällaisia voisivat olla esimerkiksi viranomaisille tuotettavat palvelut tai uusien teknologioiden kehittäminen. Suomessa on kuitenkin pitkät perinteet viranomaisten ja yritysten väliselle yhteistyölle muun muassa puolustusteollisuuden piirissä.

Laajassa merkityksessä Euroopan unionin tasolla valmistelussa olevat lainsäädäntöhankkeet, jotka koskevat tietosuoja-asetusta ja EU:n verkko- ja tietoturva-direktiiviä (NIS-direktiivi) tukevat yhteistä tietosuoja- ja tietoturvapolitiikkaa. Toteutuessaan nämä uudistukset tulevat yhdenmukaistamaan jäsenmaiden lainsäädäntöä voimakkaasti ja tämä voi parhaimmillaan nostaa EU-valtioiden kilpailukykyä kansainvälisillä digitaalisilla markkinoilla. (Kitinprami 2016, 68.)

6.3 Haastateltujen asiantuntijoiden näkemykset siviilitiedustelun vaikutuksista

Tätä tutkimusta varten haastateltiin yhteensä yhdeksää eri asiantuntijaa, jotka olivat työnsä puolesta olleet mukana tiedustelulainsäädäntöhankkeessa tai olivat yritys-, tieto- tai kyberturvallisuusalan edustajia. Pyrin valitsemaan mahdollisimman laajasti eri osa-alojen ammattilaisia, jotta saisin tarkemman kokonaiskuvan suomalaisesta tiedustelulainsäädäntöhankkeesta, jota ei juurikaan ole tutkittu aiemmin.

Haastattelu jakautui kahteen pääosa-alueeseen: siviilitiedustelulainsäädäntöhankkeeseen sekä yritysten kyberturvallisuuteen. Kysymyksillä pyrittiin muun muassa selvittämään onko valmisteilla olevalle siviilitiedusteluhankkeelle tarvetta, sisältääkö lakihanke jonkinlaisia puutteita tai haittoja yritysten liiketoiminnalle, millaisia vaikutuksia tietoliikennetiedustelulla voisi olla elinkeinoelämälle, vaikuttaako käynnissä oleva lakihanke investointipäätöksiin, onko kokonaisuuden valvonta tarpeeksi kattava sekä millaisena haastattelijat näkivät suomalaisten yritysten kyberturvallisuustason haastattelun hetkellä.

Kaikki haastatelluista olivat sitä mieltä, että Suomeen tarvitaan selkeä ja tarkoin säädelty tiedustelulainsäädäntö, jotta viranomaisilla olisi mahdollisuus saada uhkaperusteista tilannetietoa erityisesti tietoverkoissa tapahtuvista toimista, mitkä aiheuttaisivat vakavan uhkan Suomen kansalliselle turvallisuudelle. Vaikka esimerkiksi tietoliikennetiedustelukyvykkyys palvelisi ensisijaisesti viranomaisia sekä valtion ylintä päätöksentekoprosessia, niin enemmistö haastatelluista oli sitä mieltä, että laajemmassa perspektiivissä toimivaltuus hyödyttää myös elinkeinoelämää ja yrityksiä. Varsinkin, jos lainsäädännössä luodaan käytännössä toimiva mekanismi tietojen luovutukselle suojelupoliisilta yrityksille, jotka ovat joutuneet tai joutumassa esimerkiksi vakavan tietomurron tai yritysvakoilun kohteeksi.

Lainsäädäntöhankkeen valmistelussa mukana ollut virkamies kertoi, että lakihanke on ollut pitkä prosessi ja se on ollut opettavainen matka niin lainsäädäntöä valmistelleille työryhmille, elinkeinoelämälle kuin yksityisille kansalaisille. Hankkeen alkuaikoina lainsäädäntötyö oli keskittynyt ehkä liialti viranomaisten omien tarpeiden ja näkemysten ympärille, josta muun muassa elinkeinoelämä antoi lausunnoissaan palautetta. Tämän johdosta seuraavilla kierroksilla elinkeinoelämän edustustoa otettiin pysyviksi asiantuntijoiksi työryhmiin sekä hankkeen viestintää kehitettiin entistä avoimempaan suuntaan. Lopulta elinkeinoelämä siirtyi kannattamaan siviilitiedustelulainsäädäntöä, ehkäpä juuri selkeyden ja läpinäkyvyyden vuoksi.

Elinkeinoelämän näkökulmaa edustavan yritysturvallisuuden asiantuntijan mukaan yritysmaailman läsnäolo on välttämätöntä näin merkittävässä hankkeessa. Pelkästään ulkomailla tapahtuneiden viime aikaisten tiedustelullisten tapahtumien myötä on nähtävissä monenlaisia heijastevaikutuksia myös elinkeinoelämälle ja tästäkin syystä on tärkeätä, että yritysten ääni pääsee olemaan mukana. Hänen mukaansa on huomioitava myös se, että jatkossa, kun lain-

säädäntöä aletaan kehittämään, niin elinkeinoelämän edustus olisi mukana oleellisessa roolissa. Ruotsin signaalitiedustelulainsäädäntö, joka on hieman suppeampi kokonaisuus kuin nyt säädettävänä ole, on käynyt jo muutaman kerran parlamentissa tarkistettavana eli tämäkin osoittaa, että lainsäädäntö vaatii jatkuvaa seurantaa ja kehittämistä.

Yleisenä mielipiteenä asiantuntijoiden keskuudessa oli se, että kyseisestä lainsäädännöstä ja tietoliikennetiedustelusta etunenässä ei olla luomassa mitään kansallista virustorjuntajärjestelmää tietoverkon rajalle, vaan kyseessä on tiedonhankintamenetelmä. Missään tapauksessa yritysten ja organisaatioiden tarve oman tietoturva- ja kyberturvallisuusympäristön suojaamiseen ei muutu, vaan vastuu tästä säilyy yrityksillä itsellään. Tiedonhankintamielessä Suomen viranomaisten havaintokyky kasvaa ja tämän seurauksena esimerkiksi valtiollisten tai järjestäytyneen rikollisuuden suorittamat operaatiot voidaan tunnistaa entistä tehokkaammin.

Yritysturvallisuuden asiantuntijan mukaan käynnissä oleva siviilitiedustelulainsäädäntöhanke palvelee erityisesti elinkeinoelämän intressejä, mikäli viranomaisilla on mahdollisuus luovuttaa tietoa yrityksille. Ulkomaiden varsin aktiivisesti Suomessakin harjoittama taloudellinen tiedustelu ja yritysvakoilu tai tällaisten operaatioiden paljastaminen, tapahtuivatpa ne tietoverkoissa tai muualla, hyödyntää suomalaista elinkeinoelämää merkittävästi.

Haastatteluissa tuli ilmi, että yritysvakoilua sekä tietomurtoja kohdistetaan tosiasiallisesti suomalaisiin yrityksiin säännöllisesti. Kansainvälisen asiantuntijayrityksen kyberturvallisuusjohtajan, suomalaisen asiantuntijayrityksen tietoturvajohtajan sekä kyberturvallisuuspalveluita tarjoavan yrityksen kehitysjohtajan sekä johtavan tietoturvakonsultin yhteiset kokemukset osoittivat, että suomalaiset yritykset ovat jo joutuneet tällaisten tiedusteluoperaatioiden kohteiksi, mutta niistä ei välttämättä olla julkisuuteen haluttu kertoa mitään. Kyberturvallisuusjohtajan mukaan pelkästään valtiollinen yritysvakoilu on muuttanut yritysten suojautumisvaatimuksia merkittävästi. Valtiollisella tasolla voidaan puhua kyseisen toimijan armeijan tiedustelukyvykkyydestä, jolla ollaan tunkeutumassa toisessa maassa olevaan yksittäiseen yritykseen ja varastetaan sieltä luottamuksellista tietopääomaa, mikä puolestaan luovutetaan kilpailevalle yritykselle. Tässä mielessä Suomen kaltaisella maalla tulee olla kyvykkyys torjua tämänkaltaisia toimia, joilla voi olla suurta merkitystä kansantalouden näkökulmasta.

Kansainvälisen teknologiakonsernin turvallisuusjohtajan mukaan globaalissa yritystoiminnassa huomioidaan muutenkin yrityksen tiedon ja erityisesti luottamuksellisen tiedon suojaaminen. Suomessa käynnissä oleva lainsäädäntöhanke on kokonaisuutena tarkasteltuna varsin kattava ja yksityiskohtainen verrattuna niiden maiden lainsäädäntöön, jossa kyseisellä yrityksellä on toimintaa. Yrityksillä tulee olla ensisijainen vastuu oman ympäristönsä suojaamisesta. Heidän tapauksessaan haasteita lisää muun muassa hyvin laaja kansainvälinen alihankintaverkosto, joka käsittää tuhansia eri toimijoita. Turvallisuusmielessä tämä koko tuotantoketju tulee olla

mietittynä tarkkaan, jotta yritystoiminta voi suoriutua tehokkaasti ja tuloksellisesti. Samaa mieltä oli johtava tietoturvakonsultti, jonka mukaan tämä lainsäädäntö ei tule vaikuttamaan esimerkiksi kansainvälisiä konesalipalveluita tarjoavien globaalien yritysten mahdollisiin investointipäätöksiin Suomessa. Tähänkin mennessä Suomesta käsin operoivien datakeskusten liikenne menee muun muassa Ruotsissa toimivan FRA:n valvontajärjestelmien läpi, joten Suomeen tuleva vastaavanlainen tiedustelujärjestelmä olisi vain yksi lisä tässä kokonaisuudessa.

Haastatellun professorin mukaan Suomessa lainsäädäntö on laahannut digitalisaation ja siihen liittyvän turvallisuuden perässä. Hänen mukaansa se, että ylipäätänsä tiedusteluun syntyy lainsäädäntö, pelisäännöt, erilaiset valvontamekanismit, joita noudatetaan, niin se on Suomen kaltaiselle yhteiskunnalle aivan välttämätön asia. Kärjistäen voisi hänen mielestään sanoa, että tuli lainsäädännöstä millainen tahansa, niin on hyvä asia, että se tulee. Tällöin esimerkiksi ulkomaiset sijoittajat tietävät, millä pelisäännöillä tässä yhteiskunnassa toimitaan.

Yleisiä huolenaiheita liittyi muun muassa tietoliikennetiedusteluun liittyvään valvontaan ja sen tehokkuuteen. Haastatellun virkamiehen mukaan uskottava tiedustelutoiminta vaatii tehokkaan valvonnan. Hänen mukaansa valvonnan tulee tapahtua monella eri tasolla ja siihen valmistelutyössä ja lopulta hallituksen esityksessäkin on päädytty. Kattavan parlamentaarisen ja viranomaispohjaisen valvonnan lisäksi toiminnan tulee perustua tarkkaan pöytäkirjaamiseen ja laajoihin lokitietoihin, jotta tarvittaessa voidaan osoittaa, että tiedot ovat eheitä ja luottamuksellisuus on säilynyt. Lisäksi lainsäädäntötyössä on pyritty käyttämään jo valmiiksi käytössä olevia toimivaltuuksia uusien valtuuksien pohjana, koska näin toimintaan sekä sen valvontaan liittyvät ihmiset tietävät jo melko pitkälle miten juridisessa mielessä kokonaisuus toimii. Erityisesti tietoliikennetiedustelun ollessa täysin uusi toimivaltuus, vaatii se koulutusta niin operatiivisten toimijoiden kuin tuomioistuintenkin kannalta.

Useata asiantuntijaa askarrutti se, että tällä hetkellä lainsäädäntöhanke on edelleen kesken, joten esimerkiksi yritysten näkökulmasta tulevat vaikutukset eivät ole vielä tarkoin tiedossa. Yritysturvallisuuden asiantuntijan mukaan yritysten tulisi perehtyä hyvin huolellisesti tässä vaiheessa käynnissä olevaan tiedustelulainsäädäntöön, jotta ymmärrettäisiin aidosti, mitä ja mistä asioista säädetään.

7 Opinnäytetyön tulokset

Yhteiskunnan kiihtyvä digitalisaatio ja siihen olennaisesti liittyvä kybertoimintaympäristö on aiheuttanut yritysten toiminnalle aiempaa laajempia haasteita. Kyberturvallisuus tulisi nähdä yritysten johdossa strategisena kilpailutekijänä, mitä tehokkaasti hyödyntämällä yritys pystyy erottautumaan kansainvälisillä markkinoilla. Suomessa toimivan tietoturvaklusteri FISC ry:n

Juha Remeksen mukaan Suomen tavoitetta päästä Pohjoismaissa kybertutkimuksen kärkimaaksi uhkaa osaajapula. Hänen mukaansa alan koulutuspaikkoja tulisi olla kymmenkertainen määrä nykyiseen verrattuna. EU on arvioinut, että tietoturva-ala tulee työllistämään vuonna 2020 jo 350 000 ihmistä. Suomen näkökulmasta on arvioitu, että osaajatarve on noin 20 000 työntekijää. (Tekniikka & talous 2017b.)

Pyrin selvittämään opinnäytetyössä millainen käynnissä oleva siviilitiedustelulainsäädäntöhanke on erityisesti tietoliikennetiedustelun näkökulmasta. Tarkoituksena oli myös monipuolisilla asiantuntijahaastatteluilla selvittää millaisia vaikutuksia tulevalla lainsäädännöllä voisi olla yritysten liiketoiminnan kannalta, varsinkin tietointensiivisillä aloilla. Työn tavoitteena oli luoda uutta tietoa varsin vähän tutkitusta alueesta, jolla vallitsee paljon eri toimijoiden mielipiteitä niin hankkeen puolesta kuin sitä vastaankin. Olisikin tärkeätä, että asiaa tarkasteltaisiin objektiivisesti useasta eri näkökulmasta.

Tutkimus lähti liikkeelle siitä olettamasta, että yritykset eivät välttämättä näe kovin positiivisena kehityksenä, mikäli kansallinen viranomainen suorittaa edes tietoverkon rajalla tietoverkkotiedustelua. Alussa päällimmäisenä ajatuksena oli, että tiedustelumenetelmät voisivat aiheuttaa uhkia esimerkiksi rajat ylittäviä pilvi- tai konesalipalveluita käyttävien yritysten toiminnassa, koska verkoissa oleva liikenne joutuisi kulkemaan tiedustelujärjestelmän lävitse päästäkseen ulkomaille. Samalla nähtiin arveluttava se, että miten tiedusteluviranomaiset käsittelisivät saamiaan tietoja ja millainen valvontamekanismi kyseiselle kokonaisuudelle olisi riittävä.

Hyvin nopeasti kävi kuitenkin ilmi, että käynnissä olevalla lainsäädäntöhankkeella on yritysten toiminnan ja elinkeinoelämän kannalta enemmän hyötyjä kuin haittoja. Elinkeinoelämän mielipiteissä oli nähtävissä selkeä muutos ensimmäisen tiedonhankintalakityöryhmän ja siviililakityöryhmän valmistelujen sekä mietintöjen välissä. Lainsäädännön valmistelussa huomioitiin entistä paremmin yritysmaailman edustus ja tästä seuranneesta positiivisesta palautteesta oli havaintoja myös tämän tutkimuksen asiantuntijahaastatteluissa. Elinkeinoelämää edustaneen yritysturvallisuuden asiantuntijan mukaan hyvä asia oli se, että lainsäädäntötyöryhmien ja elinkeinoelämän välillä on ollut aito vuorovaikutusta, jolla monia epäilyttäviä kysymyksiä ja kokonaisuuksia on saatu hälvennetyksi.

Opinnäytetyön kautta on ollut nähtävissä Suomen yhteiskunnan erityispiirre, jossa julkisen ja yksityisen sektorin välillä on toimiva yhteistyöside. Kyseisestä yhteistyöstä voidaan käyttää niin sanottua public-private-partnership, jota haastateltu professorikin korosti. Hänen mukaansa Suomi onkin tällaisen yhteistyön hyödyntämisessä maailman parhaita, mutta tiedusteluun liittyvien kysymysten kanssa Suomi ei ole vielä maailman kärkimaita.

Haastateltujen asiantuntijayritysten mukaan heillä ei ole näkynyt, että yritykset olisivat juurikaan kohdistaneet mielenkiintoaan tiedustelulainsäädäntöä kohtaan. Kyberturvallisuusjohtajan mukaan asiasta on keskusteltu hyvin yleisellä tasolla muutamien yritysten kanssa, mutta kyse on ollut enemmänkin muodollisista kyselyistä kuin käytännön asioiden selvittämisestä. Haastatellun tietoturvajohtajan mukaan hän ei usko, että suunnitteilla oleva lainsäädäntö vaikuttaisi yritysten toimintaan millään tavalla. Yritysten tietoliikenne liikkuu eri verkkopalveluiden käytön vuoksi monien vähintään samanlaista tiedustelutoimintaa tekevien maiden lävitse, joten yritysten on pitänyt varautua tähän jo aiemmin eri suojaus- ja turvamenetelmillä. Suojausten ja salausten kasvava käyttö tulee myös aiheuttaa merkittäviä haasteita myös tiedustelutoiminnalle, koska tarkkaan tietoon ei yksinkertaisesti ole mahdollista päästä, vaan on käytettävä erilaisia metatietoja. Hän ei myöskään usko, että tällaisella lainsäädännöllä olisi mitään merkitystä ulkomaisiin investointeihin Suomessa. Todennäköisesti kaikki muut asiat kuten työvoiman saatavuus, verotusasiat ja poliittinen vakaus määräävät oikeasti, että mihin investointeja kohdistetaan.

Opinnäytetyön kirjoittamisen aikana oli havaittavissa, että haastatellut asiantuntijat sekä yleinen julkinen mielipide olivat kääntymässä hankkeen puolelle. Siviilitiedustelulainsäännöllä nähtiin olevan pelkästään positiivista puolia yritystoiminnan kannalta. Tietoliikennetiedustelun nähtiin tuovan tarpeellisen lisän, jotta viranomaisilla olisi tosiasialliset mahdollisuudet havaita ja estää ulkomaisten toimijoiden Suomessa harjoittaman yritysvakoilun tai muun vahingollisen toiminnan, mikä aiheuttaa vakavan uhkan Suomen kansalliselle turvallisuudelle.

Avoimet kysymykset näyttävät tällä hetkellä kilpistyvän kansallisen turvallisuuden määritelmään ja lainsäädännön voimaantuloon nykyisellä hallituskaudella. Alkuperäisissä valmistelua tehneiden työryhmien mietinnöissä kansallisen turvallisuuden määritelmä nähtiin eduskunnan lausuntokierroksella olevan hieman liian väljä. Aiemmin tiedustelumenetelmien käyttö perustui muun muassa määriteltyyn listaan eri tilanteista, joissa kansallinen turvallisuus olisi uhattuna. Lakiehdotukseen on tulossa merkittävä tiukennus, jonka mukaan suojelupoliisin tulee antaa tarkempi tietoja tiedustelutoiminnasta ja sen kohteista. Lisäksi suojelupoliisin tulisi pystyä osoittamaan selkeästi, millaisen konkreettisen uhkan käynnissä oleva toiminta aiheuttaisi kansalliselle turvallisuudelle. (Yleisradio 2017b.)

Tutkimusta varten haastatellun yliopiston professorin mukaan yhteiskunnan kannalta turvallisuus on aina kulttuurinen asia, mihin tulee panostaa entistä enemmän toimintaympäristön muutoksenkin vuoksi. Hänen mukaansa tulevaisuudessa tulisi pyrkiä puhumaan enemmän turvallisuudesta kokonaisuutena kuin yksittäisistä turvallisuuden aloista kuin esimerkiksi kyberturvallisuudesta tai tietoturvallisuudesta. Turvallisuuden tulisi olla opittua ja tämä kulttuurimuutos vie aikaa. Ensinnäkin tulisi panostaa siihen, että laitettaisiin turvallisuuden näkökulmasta perusasiat ensin kuntoon, koska tälläkin hetkellä suurimmat yritysten turvallisuusuhat

kohdistuvat ihmisiin, heidän piittaamattomuuteen sekä heikkoon tietoisuuteen. Teknisessä mielessä yritysten tulisi panostaa tietoteknisen infrastruktuurin perustan ylläpitoon ja päivittämiseen. Tutkimusyhtiö Gartnerin vuonna 2016 tekemän ennusteen mukaan vuoteen 2020 menneessä edelleen noin 99 prosenttia tehdyistä tietomurroista tehdään käyttäen yleisesti tiedossa olevia haavoittuvuuksia (Gartner 2016, 2.)

Haastattelujen perusteella oli nähtävissä, että kyberturvallisuusalan koulutusta ja osaamista tulisi kehittää Suomessa. Yritysturvallisuuden asiantuntijan mukaan kokonaisuus lähtee koulutuspoliittiselta tasolta eli Suomeen ylipäätänsä tarvittaisiin runsaasti digitaalisen ajan osaajia, joista turvallisuusosaajien alue olisi vain yksi. Yksityisen sektorin asiantuntijayritykset kertoivat, että ne ovat pitkään jo rekrytoineet ja kouluttaneet itse tarvitsemiaan asiantuntijoita, vaikka tämä tapa on aikaa vievää ja kallista. Kokonaisuuden kannalta ei tarvita pelkästään teknistä syväosaamista, vaan tarvitaan muun muassa erilaista tuote- ja ratkaisuosaamista, johtamisosaamista sekä viestintätaitoja. Tietoturvajohtaja kritisoi hieman kyberturvallisuuteen liittyvän koulutuksen tasoa Suomessa. Esimerkkinä hän käytti muun muassa Hollantia, jossa he pystyvät rekrytoimaan valmiita asiantuntijoita suoraan koulusta työelämän tarpeisiin. Suomessa korkeakouluista valmistuneita työntekijöitä tulee usein lisäkouluttaa, jotta pystyttäisiin vastaamaan työelämän asettamiin tarpeisiin.

7.1 Johtopäätökset

Eduskunnan hallintovaliokunta antoi lausuntonsa (HaVL 7/2018 vp) liittyen perustuslain kymmenennen pykälän muuttamisesta, jossa säänellään luottamuksellisen viestin salaisuuden suojasta. Lausunnon yhteenvedossa todetaan, että Suomen turvallisuuspoliittinen toimintaympäristö on muuttunut monella eri tavalla. Erityisesti kyberuhkat ovat muuttaneet muotoaan ja ovat nykyisellään vaikutuksiltaan aiempaa moninaisempia sekä haitallisempia niin yksittäisille kansalaisille, yrityksille kuin suomalaiselle yhteiskunnalle.

Samaisessa hallintovaliokunnan lausunnossa mainitaan, että kansallisella kyberkyvykkyydellä on tulevaisuudessa entistä keskeisempi merkitys maan kokonaisturvallisuuden ja yhteiskunnan kriittisten toimintojen ja turvaamisen sekä Suomen kilpailukyvyn kannalta. Suomi on yksi maailman digitalisoituneimmista yhteiskunnista. Tällä hetkellä lainsäädäntö ei huomioi kybertoimintaympäristöön liittyviä erityispiirteitä. Näistä syistä onkin erityisen tärkeätä luoda nopealla aikajänteellä säädöstä sekä menetelmiä, joilla parannetaan kyberuhkiin liittyvää torjunta- ja ennakointikykyä. Valiokunnan johtopäätöksenä lausutaan, että Suomen tarvitaan uutta lainsäädäntöä, joka mahdollistaa toimivaltaisille viranomaisille tehokkaan tiedustelutiedon hankinnan. (HaVL 7/2018 vp.)

Kuten Saara Jantunen mainitsee kirjassaan, tulisi julkisessa keskustelussa turvallisuusympäristön muutoksesta puhua oikeilla nimillä ja käsitteillä. Todellisuutta ei tulisi muuntaa sellaiseksi, millaisena sen haluaisimme nähdä. Tosiasia on tällä hetkellä se, että yhteiskuntamme antaa mahdollisuuden valjastaa sen perusarvot vihamielisen toiminnan käyttöön ja muun muassa Ukrainan kriisin myötä on saatu esimakua siitä, että näin myös voidaan tehdä. (Jantunen 2016, 62.)

Eduskunnan hallintovaliokunnan lausunnon (HaVL 7/2018 vp) mukaan Suomen ulkoinen turvallisuusympäristö on viime vuosina voimakkaasti heikentynyt. Suomen lähialueiden turvallisuustilanne on myöskin jatkuvasti heikentynyt sitä mukaa kuin kansainväliset poliittiset jännitteet ovat ulottuneet aiempaa pohjoisemmaksi. Perinteisen vakoilun rinnalle on noussut kybervakoilu, jossa valtiollinen toimija voi ilman merkittävää riskiä kiinnijäämisestä hankkia erittäin suuria määriä kohdevaltion turvallisuutta vahingoittavia tietoja. (HaVL 7/2018, 8.)

Suomen välilukuun suhteutettuna Suomeen pysyvästi sijoitettujen ulkomaalaisten tiedusteluupseereiden määrä on yksi maailman suurimmista länsimaissa. Ulkomaisen tiedustelun keskeisimpiin päämääriin kuuluvat Suomen politiikan ennakoiminen ja päätöksiin vaikuttaminen. Kiinnostusta herättävät myös Suomen poliittisen johdon ja väestön suhtautuminen mahdolliseen Nato-jäsenyyteen, Suomen energiapoliittiset päätökset ja energiahuoltovarmuus sekä Suomen kyberturvallisuusrakenteet. (HaVL 7/2018, 10.)

Opinnäytetyön johtopäätöksenä voidaan todeta, että käynnissä oleva tiedustelulainsäädäntöhanke on suomalaisen yhteiskunnan turvallisuuden kannalta merkittävässä roolissa. Kaikki haastatellut asiantuntijat olivat sitä mieltä, että tiedustelulainsäädäännölle on selkeä tarve. Nykyisellään käytävässä poliittisessa keskustelussa korostuu lainsäätämisen aikataulu. Kansallisen turvallisuuden parantamisen kannalta tiedustelulait tulisi saattaa voimaan mahdollisimman nopeasti, koska mikäli suunnitellut lakimuutokset tulevat voimaan vasta seuraavan hallituksen aikana, saadaan tiedustelutoimivaltuudet käytännössä käyttöön vasta vuoden 2020 jälkeen. Muussa tapauksessa tiedustelukyvykkyysiä voitaisiin alkaa kehittää jo vuoden 2018 loppupuolella.

Suomessa ei ole aiemmin ollut lainsäädäntöä tiedustelutoimintaan ja tästä syystä viranomaisten toimintamahdollisuudet havaita, ehkäistä ja torjua yhteiskuntaa uhkaavista vakavista teoista ovat olleet vajavaiset. Aiemmin toimivaltuudet ovat keskittyneet rikostorjunnan tarpeisiin, jolloin toimivaltuuksien käyttö perustuu yksittäiseen tekoon ja siihen liittyvään epäiltyyn. Käynnissä olevalla siviilitiedustelulainsäädännöllä pyritään luomaan mahdollisuuksia hankkia tietoa uhkaperusteista tietoa eri toimista ja ilmiöistä.

Huomionarvoista on kuitenkin se, että vaikkakin tämänhetkiset tulokset osoittavat, ettei siviilitiedustelulainsäädännöstä tai erityisesti tietoliikennetiedustelusta ole nähtävissä juurikaan negatiivisia vaikutuksia yritystoimintaan, niin kyse on vielä vahvistamattomasta lainsäädännöstä. Poliittinen kiinnostus ja osittainen näkemysero poliittisten puolueiden välillä velloo edelleen ja tällä hetkellä ei ole selkeätä tietoa, koska tiedustelulakikokonaisuus tulisi voimaan. Hyvin todennäköisesti hallituksen tekemään esitykseen (HE 202/2017 vp) ei ole tulossa merkittäviä sisällöllisiä muutoksia, mutta erityisesti yksityisyyden suojaan sekä perustuslain muuttamiseen liittyvät kysymykset viivästyttävät lain säätämisen aikataulua. Kärjistettynä voidaan todeta, että tiedustelulainsäädäntöön liittyy tällä hetkellä paljon spekulaatiota ja vasta säädetty lakikokonaisuus tulee osoittamaan lopullisen suunnan.

Opinnäytetyöhön haastatellun professorin mukaan lain voimaantulon jälkeen nähdään vasta millaiseksi käytäntö muotoutuu ja ovatko muun muassa lain valvontakeinot riittäviä. Vaikkakin asia on itsestään selvää, niin ei voida ajatella, että välittömästi lainsäädännön voimaantulon jälkeen tilanne muuttuisi paremmaksi ja viranomaiset havaitsisivat mitä tietoverkoissa tapahtuu. Käytännön kokemukset tulevat osoittamaan, että miten suunnitellut toimintamallit ja tiedonkulku tulee toimimaan.

Vihreiden eduskuntaryhmän mukaan Suomen tulee ottaa mallia ja oppia muiden maiden tekemistä virheistä liittyen tiedustelutoimintaan. Esimerkiksi Ruotsin FRA-lakia muutettiin tiukemmaksi sen jälkeen, kun huomattiin sen loukkaavan yksityisyyttä liikaa. (Verkkouutiset 2018b.) Yleisenä johtopäätöksenä voidaankin todeta, että niin tietoliikennetiedustelun ja yleisesti tiedustelulainsäädännön voimaantulon jälkeen on oltava mahdollisuus tarkentaa lainsäädäntöä käytännön kokemusten perusteella. Lakikokonaisuuteen liittyy paljon niin lainsäädännöllistä kuin teknistäkin problematiikkaa ja tämän vuoksi asiantuntijoiden käyttöä tulisi tehostaa myös tulevaisuudessa.

Siviilitiedustelulainsäädäntöä valmistelleen työryhmän avoimuus, läpinäkyvyys sekä viestinnän kehittäminen on ollut oleellista siinä, että elinkeinoelämän mielipide on muuttunut erityisesti tiedustelulainsäädäntöä tukevaksi. Vaikkei viranomaisten rooliin kuulukaan vastata muun muassa yritysten turvallisuudesta, niin tietoliikennetiedustelutoimivaltuudella voidaan olettaa olevan suuri merkitys suomalaisen tietoverkottuneen yhteiskunnan entistä paremman suojaamisen näkökulmasta. Lainsäädäntötyössä olleen virkamiehen mukaan tietoliikennetiedustelun tehokkuudesta voi olla montaa mieltä, mutta Ruotsin poliisin tiedustelu- ja turvallisuuspalvelu Säpon (Säkerhetspolisen) päällikön mukaan he ovat pystyneet estämään kaksi terroristi-iskua nimenomaan tietoliikennetiedustelun avulla. Pohdittavaksi jää, että mikäli kyseisellä toimivaltuudella voitaisiin estää yksikin konkreettinen isku, niin olisiko toimivaltuus ehkä maksanut itsensä ikään kuin takaisin. Mikäli viranomaisilla ei olisi tällaisia toimivaltuuksia ja maahan

kohdistuisi terroristi-isku, niin ei olisi täysin oikeutettua kysyä, että miksi viranomaiset eivät tehneet mitään.

Puolustusvoimien tiedonhankintalakityöryhmän mietintö kuvastaa hyvin tämänkin opinnäytetyön johtopäätöksiä liittyen tiedustelulainsäädäntöhankkeeseen sekä tietoliikennetiedusteluun. Tiedustelun kautta tehtävän tiedonhankinnan ja tietoliikennetiedustelun tarkoituksena on hankkia kansallisen turvallisuuden kannalta välttämätöntä tiedustelutietoa vakavista kansainvälisistä uhkista. Toiminnalla olisi tarkoitus tukea valtion ylimmän johdon päätöksentekoa ja varmistaa sen perustuminen oikeaan, ajantasaiseen sekä luotettavaan tietoon.(Puolustusministeriö 2015b, 80.)

Toiminnalla myös mahdollistettaisiin toimivaltaisten viranomaisten ryhtyminen uhkien torjuntaan. Tietoliikennetiedustelussa tulisi huomioida tarkasti ihmis- ja perusoikeudet ja sen vaikutuksia arvioitaessa tulisi huomioida vaikutukset yhteiskunnan digitalisoitumiseen ja yritysten toimintaedellytyksiin. Elinkeinopoliittiset ja digitaalisen ekosysteemin kehitykseen vaikuttavat tekijät tulisi huomioida erityisen tarkasti. Lainsäädäntöön liittyvässä jatkotyössä on pohdittava kattavasti tietoliikennetiedustelun teknisiä eri käytännön toteuttamistapoja ja niiden taloudellisia vaikutuksia. (Puolustusministeriö 2015b, 80.)

7.2 Työn pohdinta

Opinnäytetyö kasvatti entisestään omaa kiinnostusta liittyen yhteiskunnan digitalisaatiokehitykseen ja siihen liittyviin turvallisuuskysymyksiin. Nykyisellään yhteiskunnan toimintoja on siirtynyt täysin kyberympäristöihin ja oma viestintämme sekä tapamme toimia yhteiskunnan jäseninä on digitalisoitunut. Tästä syystä tulee myös tiedustelulainsäädäntöä sekä tietoliikennetiedustelun merkitystä pohtia yritystoiminnassa. Kokonaisuutta voisi tarkastella paljolti turvallisuusviranomaisten näkökulmasta, mutta oleellista olisi myös arvioida kyseessä olevien merkityksellisten lainsäädäntömuutosten vaikutuksia yhteiskunnan muihinkin toimintoihin, kuten elinkeinoelämään.

Opinnäytetyön kirjoittamisen näkökulmasta tiedustelulakihankkeeseen liittyvää kokonaisuutta oli lainvalmistelun keskeneräisyydestä johtuen vaikeaa hallita ja suurin osa saatavasta aineistosta keskittyi eritoten median välittämiin tietoihin. Julkisessa keskustelussa ohitettiin tärkeitä kysymyksiä, vaikkakin yksityisyyden suoja ja mahdollisen massavalvonnan olemassaolo eivät olleet yhtään vähäteltäviä asioita. Lainsäädännön valmistelun kannalta olisi ollut hyvä käydä laajemmin läpi, että millaisia vaikutuksia ja mahdollisia hyötyjä esimerkiksi tietoverkkotiedustelu tuo kansallisen turvallisuuden parantamisen näkökulmasta niin kansalaisille, yrityksille kuin koko yhteiskunnalle. Yleisesti voidaan todeta, että melko absurdia, ettei Suomen

kaltaisella korkean teknologian kärkimaana ollut minkäänlaista lainsäädäntöä tiedustelutoimintaan tai vakavien uhkien torjuntaan.

Hyvänä ja ehkäpä hieman nolonakin esimerkkinä näistä puutteista oli ulkoministeriön, vuonna 2013 paljastunut valtiollisen tahon tietomurto, joka oli jatkunut todennäköisesti vuosikausia ja vasta Ruotsin tiedusteluviranomaisilta saatu vinkki lopetti kyseisen operaation. Viranomaisten niukkasanainen viestintä tapahtuneesta on toki ymmärrettävää osittain poliittisistakin syistä, ettei ulkomaisten tahojen suorittamasta tiedustelutoiminnasta ja vakoilusta haluta juuri julkisuudessa keskustella, mutta tiedustelulainsäädännön valmistelun aikana julkisesta keskustelusta on puuttunut tämä aspekti. Useat asiantuntijat ovat sitä mieltä, että terroristisen toiminnan torjunnan sijasta suurempi uhka tuleekin juuri tietoverkoissa tapahtuvasta vakoilusta.

Käytetyn aineiston sekä tehtyjen haastatteluiden perustella herää kysymys siitä, että ovatko ihmiset tänä sosiaalisen median aikakautena osin tiedostamatta luopuneet ainakin digitaalisesta yksityisyydestään. Yleisessä tiedossa on, että eri sosiaalisen median palveluita tarjoavat yritykset hyödyntävät käyttäjien tietoja muun muassa markkinoinnissa tai muun viestinnän kohdentamisessa. Viimeisenä osoituksena tästä voidaan nähdä Cambridge Analytica -yrityksen noin 87 miljoonan Facebook-käyttäjän tiedon väärinkäyttö liittyen Yhdysvaltain presidentinvaaleissa vuonna 2016 (Savon Sanomat 2018). Lisäksi näiden palveluiden ja ylipäätänsä internetissä tapahtuva liikennöinti kulkee monien tietoverkkotiedustelua harjoittavien maiden tietoverkkojen läpi, joten on miltei outoa, jos suomalaisille viranomaisille ei annettaisi toimivaltuuksia ja näkyvyyttä kotimaan tietoverkossa tapahtuvaan toimintaan, varsinkin kun toimivaltuudet ovat hyvin rajattuja.

Tähän työhön haastateltu kyberturvallisuusjohtaja tiivisti tiedustelulainsäädäntöön liittyvän kysymyksen hyvin. Kärjistettynä voisi sanoa, että tällä hetkellä viranomaisille ollaan säätämässä samantyyppisiä valtuuksia tehdä samaa, kuin mitä sosiaalisen median Facebook tai Google tekevät joka tapauksessa ja vielä paljon syvemmin. Samalla on syytä siteerata haastateltua kehitysjohtajaa, jonka mukaan viranomaisilla tulisi olla yhtäläiset toimivaltuudet digitaalisen maailman puolella kuin fyysisessä maailmassa. Maailma on digitalisoitumassa entistä nopeammin ja muun muassa talous ja rahaliikenne on digitalisoitunut, joten tämä on näkynyt myös rikollisuuden voimakkaana digitalisoitumisena. Hän kysyykin, että minkä takia internet tai tietoverkot pitäisi pyhittää rikollisten pelikentäksi?

Yritysten näkökulmasta liiketoiminnan digitalisoituminen vaatii entisestään yrityksen omia kyvykkyyksiä suojata omaa toimintaansa ja täten luoda kilpailukykyä muihin nähden. Yritysten omia kyberturvallisuuden tarpeita tai turvallisuutta ylipäätänsä ei voida ulkoistaa, vaan nykyisellään tietoliikennetiedustelu voisi toimia vain ikään kuin lisäkerroksena erilaisen tilannetie-

don kehittämisessä. Opinnäytetyön kautta on nähtävissä selkeästi, ettei lainsäädäntö valmistuessaan tule tuomaan vastauksia niin yrityksille tai viranomaisille. Vasta tämän jälkeen on luotu pelikenttä ja ne säännöt, missä kyseisiä toimivaltuuksia ja kyvykkyyksiä voidaan alkaa hyödyntämään. Tulevaisuus tulee näyttämään miten tiedustelulainsäädäntöä sekä tietoverkoissa tapahtuvaa tiedustelua täytyy kehittää, mutta oleellista on, että tähän kehitystyöhön osallistetaan niin julkisen kuin yksityisenkin puolen toimijoita.

7.3 Kooste tietoliikennetiedustelusta yrityksille

Hallituksen esityksen (202/2017 vp) mukaan Suomen turvallisuusympäristö on muuttunut sekä digitalisoitunut viime vuosina. Digitalisaatiokehitys on näkynyt myös yritysten liiketoiminnasta, mistä suurin osa nykyisellään on riippuvainen tietojärjestelmistä ja tietoverkoista. Suomen elinkeinoelämä ja talous on myös muuttunut entistä innovaatiolähtöisemmäksi, jossa korostuvat osaamis- ja teknologiaintensiiviset alat. Tällä hetkellä Suomen erityinen vahvuus kovenevassa globaalissa kilpailussa liittyy korkeatasoiseen informaatio- ja viestintäteknologiaan. Näistä syistä tietointensiivisen teollisuuden kansantaloudellinen merkitys on kasvussa. Nykyisellään Suomessa ei ole lainsäädäntöä tiedustelutoimintaan, joten esimerkiksi suojelupoliisilla ei ole tällä hetkellä toimivaltuuksia hankkia valtion turvallisuuteen liittyvää uhkatietoa. Elinkeinoelämän keskusliiton Mika Susi mainitsee esityksessään (Susi 2017), että tiedustelutoiminta olisikin tärkeätä saada sääntelyn piiriin, koska muussa tapauksessa tähän osa-alueeseen liittyvä epävarmuus tulee heijastumaan yritysten toimintaedellytyksiin ja investointeihin. Yritysten ja elinkeinoelämän kannalta on tärkeätä, että sen toimintaympäristön lainsäädäntö on vakaalla pohjalla ja muun muassa tiedusteluun liittyvät pelisäännöt ovat selkeitä.

Siviilitiedustelulakityöryhmän mietinnön mukaan tietoliikennetiedustelun käyttöön liittyy mittava määrä erilaisia kontrolleja, joiden olemassaololla varmistetaan tiedustelukeinojen lupaehtojen mukainen käyttö. Suojelupoliisi voisi tuomioistuimen lupapäätöksen ehtojen mukaisesti käyttää tietoliikennetiedustelua varsin rajatuissa tapauksissa. Mietinnön mukaan tietoliikennetiedustelulla tarkoitettaisiin Suomen rajan viestintäverkossa ylittävään tietoliikenteeseen kohdistuvaa, tietoliikenteen automatisoituun erotteluun perustuvaa teknistä tiedonhankintaa sekä tiedon käsittelyä. Tiedustelumenetelmä koskisi siis ainoastaan sellaista tietoliikennettä, joka siirtyisi suomalaisesta verkosta ulkomaiseen verkkoon ja päinvastoin. Merkittävä osa suomalaisesta tietoliikenteestä olisi jo näin rajattu tietoliikennetiedustelun ulkopuolelle. (Sisäministeriön julkaisu 8/2017, 138.)

Elinkeinoelämän näkökulmasta on toivottavaa, että tällainen hanke ei saa missään tapauksessa madaltaa yritys- tai liikesalaisuuden tasoa. Käynnissä oleva siviilitiedustelulakihanke ja erityisesti sen sisältämä tietoliikennetiedustelu ei sellaisenaan tuo yritysten toiminnan kannalta

pakottavia muutoksia viranomaisten kannalta. Yrityksiä ei velvoiteta luovuttamaan salaisavaimiaan, asentamaan takaportteja järjestelmiinsä tai muutenkaan heikentämään omaa turvallisuusinfrastruktuuriaan millään tavalla. Lainsäädäntöä valmistelleet ryhmät ovat viestineet tästä hyvin avoimesti ja läpinäkyvästi.

Vaikka yrityksille ei ole kyseisen lainsäädännön kautta tulossa velvoitteita (pl. tiedonsiirtäjät), tulisi jokaisen yrityksen perehtyä käynnissä olevaan lainsäädäntöhankkeeseen. Erityisesti niiden yritysten, joiden toiminta linkittyy kriittisen infrastruktuurin tai huoltovarmuuskriittisten palveluiden tuottamiseen, tulisi varmistua siitä, että niiden kokonaisturvallisuusinfrastruktuuri on ajan tasalla ja sitä kehitetään jatkuvasti. Lainsäädännössä mainittu tiedonluovutusmekanismi voi toimiessaan tuoda merkittäviä parannuksia ja hyötyjä, mikäli viranomaiset voivat tiedottaa tietomurron tai vakoilun kohteeksi joutunutta yritystä havaitsemistaan turvallisuuspoikkeamistaan.

Kyberturvallisuuden lähtökohdista yritysten tulisi huomioida kaikessa liiketoiminnassaan turvallisuusnäkökulmat jokaisella tasolla ja hyödyntää turvallisuus yhtenä kilpailukykyä edistävänä tekijänä. Valmistautuessaan tiedustelulainsäädännön voimaantuloon yritysten tulisi huomioida vähintään alla olevat kohdata turvallisuutensa kannalta:

1. Tee kyberturvallisuudesta koko yrityksen asia strategisesta johdosta aina työntekijöihin saakka.
2. Tunne ydinliiketoiminnan kannalta kriittinen tieto ja suojaa se asianmukaisesti.
3. Varmista, että yrityksen kokonaisturvallisuus on korkealla tasolla ja pyri testaamaan turvamekanismien toimivuutta säännöllisesti. Huomioi erityisesti tiedon ja tietoliikenteen salaus.
4. Luo selkeät prosessit ja toimintatavat, joilla tietomurto tai yritysvakoilu pyritään havaitsemaan sekä miten toimitaan, kun huomataan yrityksen joutuneen tällaisen toiminnon kohteeksi.
5. Kehitä yrityksen kyberturvallisuuden tilannetietoisuutta ja havaintokykyä, jotta yritys pystyy tarvittaessa tekemään oikeita päätöksiä sekä vastatoimia.
6. Varmista toimivat yhteyskanavat viranomaisten suuntaan ja hyödynnä esimerkiksi Kyberturvallisuuskeskuksen antamia uhkatietoja.
7. Kriittiseen infrastruktuuriin tai huoltovarmuuskriittiseen toimintaan liittyvien yritysten kannattaa hyödyntää viranomaisten lisäpalveluita (esimerkiksi HAVARO).
8. Ohjeista ja lisää henkilöstön kyberturvallisuustietoutta.

Mikäli yrityksessä yllä olevassa listauksessa olevia asioita on kehitetty jo aiemmin, ei tiedustelulainsäädännön tuomat vaikutukset ole kovin suuria. Organisaatioissa tulisi pyrkiä kehittämään toiminnan sietokykyä erityisesti poikkeustilanteita varten. Tämänkaltaisissa tilanteissa

tulisi olla käytössä selkeät ja valmiiksi suunnitellut sekä harjoitellut prosessit, millä toiminnot voidaan palauttaa mahdollisimmin lähelle normaalia toimintaa. Yritysten tulisi luoda tarpeen mukaan yhteistyöverkostot tarvittaviin viranomaisiin, jotta tietomurron tai muun toimintaa vakavasti haittaavan tapahtuman ilmetessä yrityksellä olisi käytössä paras mahdollinen apu. Erityisesti huoltovarmuuden kannalta kriittisten yritysten tulisi olla yhteydessä Kyberturvallisuuskeskukseen tai Huoltovarmuuskeskukseen, joista on mahdollista saada korkeatasoista ohjeistusta toiminnan turvaamiseen.

Yritysten kannalta selkeä ja läpinäkyvä lainsäädäntö poistaa spekulaatioita ja epävarmuutta. Lisäksi parempi tilannekuva edistää Suomen kaltaisen pienen maan menestymismahdollisuuksia globaalissa ympäristössä. Ulkomaisten investointien kannalta selkeä lainsäädäntö edesauttaa uusien investointien tekemistä. Huomioitavaa on myös se, että elinkeinoelämä tulee nähdä osana kansallista turvallisuutta, mitä tulee suojata myös viranomaistasolla. Tiedustelulainsäädäntö voi myös synnyttää kokonaan uutta liiketoimintaa, koska viranomaiset tulevat todennäköisesti tarvitsemaan erilaisia palveluita, osaamista ja teknologiaa yrityksiltä. (Susi 2017.)

7.4 Jatkotutkimustarpeet sekä kehitysehdotukset

Tällä hetkellä tiedustelulainsäädäntöön liittyvälle tutkimukselle on suuri tarve, koska tämä tutkimus ei tarkastele aihekokonaisuutta voimaantulleen lainsäädännön kannalta. Tiedustelulakikokonaisuuden lopullista muotoa ja sen käytännön toteutumista tulisi tarkastella niin yhteiskunnan yleisen turvallisuuskehityksen, yksilöiden kuin elinkeinoelämän näkökulmista. Lainsäädännön voimaantulon jälkeen tulisi tutkia, että muuttivatko suomalaiset yritykset joitakin toimintatapojansa erityisesti tietoliikennetiedustelun vuoksi ja onko kyseisellä lainsäädännöllä ollut käytännön vaikutuksia ulkomaisten tekemiin sijoituksiin Suomessa.

Tiedustelutoiminnan kansainvälistä tutkimusta tulisi osin soveltaa suomalaisen tiedustelulainsäädännön tutkimuksessa, mutta se ei sellaisenaan sovellu pelkästään jo lainsäädännön erilaisuuden vuoksi. Elinkeinoelämän vaikutuksia tarkasteltaessa tosin kansainväliset tutkimukset voisivat tuottaa suurtakin lisäarvoa kotimaiselle tutkimukselle, jotta investointien toteutumista voitaisiin verrata laajallakin perspektiivillä. Kaiken kaikkiaan tiedustelutoiminta on laaja tutkimuskenttä, jonka tutkimusta tulisi kehittää ja tutkimusta tulisi rajata niin viranomaisten kuin yksityisen sektorin tarpeiden mukaan.

Lainsäätäjän tulisi huomioida tiedustelulakikokonaisuutta voimaansaattaessa, että Suomen yhteiskunnan toimivuuden kannalta elinkeinoelämän ja yritysten merkitys korostuu. Tällä hetkellä suuri osa kriittisen infrastruktuurin palveluista tuotetaan yksityisen sektorin toimesta. Tiedustelulainsäädännön valmistelussa on huomioitu elinkeinoelämää melko hyvin, mutta yritysvaikutukset ovat edelleen varsin yleisellä tasolla. Erityisen merkityksellistä olisi luoda toi-

miva mekanismi viranomaisten ja yksityisen sektorin toimijoiden välillä, jotta viranomaisilla olisi tosiasialliset mahdollisuudet tiedustelutoimintaa vaarantamatta luovuttaa yrityksille tietoja, mikäli jossain yrityksessä havaittaisiin epätoivottua toimintaa tai uhkaa.

Tiedustelulainsäädäntöön liittyvää julkista keskustelua tulisi kohdistaa yksityisyydensuojan ja massavalvonnan kysymyksistä kansantalouden turvaamiseen. Viranomaiset ja yksityinen sektori on osoittanut, että nykyisellään suomalaisiin yrityksiin ja valtionhallinnon toimijoihin kohdistuu valtiollista vakoilua, joka voi vaarantaa vakavasti Suomen kansallista turvallisuutta. Laainsäädännöllisesti tulisi luoda puitteet ja toimintatavat, millä viranomaisilla ja elinkeinoelämällä olisi yhteiset ohjeistukset tai toimintatavat miten toimitaan, jos kuka tahansa havaitsee tietomurron tai yritysvakoilua. Yrityksille tulisi luoda luottamuksellinen kanava tiedottaa viranomaisia, mikäli ne ovat joutuneet vakoilutoiminnan kohteeksi, koska muun muassa mainetappioista ja muista taloudellisista menetyksistä johtuen yritykset eivät mielellään tuo näitä asioita julkisuuteen.

Käynnissä olevaa tiedustelukokonaisuutta tulisi tarkastella myös yhteiskunnan kyberturvallisuuden kannalta. Valtioneuvoston kanslian Suomen kyberturvallisuuden nykytilaa, tavoitetilaa sekä tarvittavia toimenpiteitä tavoitetilan saavuttamiseksi läpikäydyn julkaisun mukaan kyberturvallisuus on kehittynyt viime vuosina kansallisen kyberturvallisuusstrategian linjausten sekä laaditun toimenpanosuunnitelman perusteella. Julkaisun tutkimuksen mukaan tarvitaan merkittäviä kehittämistoimenpiteitä, jotta voidaan saavuttaa edelläkävijyyden asema kyberturvallisuudessa. Tunnistettuja kehittämiskohteita julkaisussa olivat muun muassa strategisen johtamisen kehittäminen, poliittisen sitoutumisen vahvistaminen, kansainvälisen toiminnan tehostaminen, tilanne- ja havaintokyvyn parantaminen, elintärkeiden toimintojen turvaamisen edistäminen, lainsäädännön kehittäminen, osaamisen sekä tutkimuksen ja yleisen tietoisuuden vahvistaminen. (Valtioneuvoston kanslia 2017, 2.)

Lähteet

Kirjalliset lähteet

Anttola, N., Takkunen, J. 2016. Suomi valtiollisen tiedustelun kynnyksellä: jatkotutkimus tiedustelulainsäädännön vaikutuksista sisäisen turvallisuuden viranomaiskentässä. Espoo: Laurea-ammattikorkeakoulu.

Helsingin seudun kauppakamari. 2015. Yrityksiin kohdistuvat kyberuhat 2015. Helsinki: Helsingin seudun kauppakamari.

Hirsjärvi, S., Hurme, H. 2014. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus.

Hirsjärvi, S., Remes, P., Sajavaara, P. 2009. Tutki ja kirjoita. Helsinki: Tammi.

Jantunen, S. 2016. Infosota. Helsinki: Otava.

Keskuskauppakamari. 2017. Yritysten rikosturvallisuus 2017. Helsinki: Keskuskauppakari.

Kitinprami, I. 2016. Suomi, tiedon turvasatama? Helsinki: Aalto-yliopisto.

Limnéll, J., Majewski, K., Salminen, M. 2014. Kyberturvallisuus. Jyväskylä: Docendo.

Oittinen, A. 2017. Yrityssalaisuuksiin kohdistuvat loukkaukset ja kyberrikollisuus. Rovaniemi: Lapin yliopisto.

Ruusuvuori, J., Tiittula, L. (toim.) 2005. Haastattelu - tutkimus, tilanteet ja vuorovaikutus. Tampere: Vastapaino.

Tiilikainen, H. 2015. Hybridisota: rintamaraportti. Helsinki: Auditorium.

Tuomi, J., Sarajärvi, A. 2012. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Tammi.

Vapaavuori, T. 2016. Yrityssalaisuudet, liikesalaisuudet ja salassapitosopimukset. Helsinki: Talentum Pro

Sähköiset lähteet

BBC News. 2012. Alan Turing: The codebreaker who saved millions of lives. Viitattu 26.5.2018. http://www.bbc.com/news/technology-18419691

Data Center Dynamics. 2014. Facebook to build second data center in Sweden. Viitattu 3.4.2018. http://www.datacenterdynamics.com/content-tracks/design-build/facebook-to-build-second-data-center-in-sweden/85409.fullarticle

Eduskunta. 2018. Tiedustelulait. Viitattu 26. 5.2018. https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/tiedustelulait.aspx.

Effi - Electronic Frontier Finland ry. 2017. Effin lausunto siviilitiedustelulaista. Viitattu 27.3.2018. https://effi.org/lausunto-siviilitiedustelu-2017-06-16

Elinkeinoelämän keskusliitto. 2017. Tiedustelu on tärkeätä saada sääntelyn piiriin. Viitattu 29.3.2018. https://ek.fi/ajankohtaista/tiedotteet/2017/04/19/tiedustelu-on-tarkeaa-saada-saantelyn-piiriin/

Elinkeinoelämän tutkimuslaitos - Etla. 2016. Suurten yritysten ja niiden arvoketjujen rooli taloudessa. Helsinki: Elinkeinoelämän tutkimuslaitos. Viitattu 7.4.2018. https://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-53.pdf

FiCom - Tietoliikenteen ja tietotekniikan keskusliitto. 2017. Tietoliikennetoimiala tiedustelulakipaketista: Mittava kokonaisuus, joka edellyttää tarkempaa analyysiä. Viitattu 26.3.2018. https://www.ficom.fi/ajankohtaista/uutiset/tietoliikennetoimiala-tiedustelulakipaketista-mittava-kokonaisuus-joka

FISC - Finnish Information Security Cluster ry. 2017. Tiedustelulainsäädäntöä tarvitaan Suomessa. Viitattu 20.3.2018. https://www.fisc.fi/tiedote-tiedustelulainsaantoa-tarvitaan-suomessa/

Fortune. 2017. Amazon Cloud Goes Nordic. Viitattu 3.4.2018. http://fortune.com/2017/04/04/aws-swedish-data-center/

Gartner Inc. 2016. Gartner's Top 10 Security Predictions 2016. Viitattu 6.4.2018. https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/

Helsingin Sanomat. 2013. Ulkoministeriön verkko oli täysin ulkopuolisten hallussa. Viitattu 15.2.2018. https://www.hs.fi/kotimaa/art-2000002685298.html

Helsingin Sanomat. 2014. EK torjuu Suomeen suunnitellun tiedustelulain. Viitattu 27.3.2018. https://www.hs.fi/talous/art-2000002715994.html

Kasvi, J. 2017. Tiedusteltua tiedustelua. Viitattu 28.3.2018. https://www.slideshare.net/JyrkiKasvi/tiedusteltua-tiedustelua

Karjalainen. 2017. Risikko tiedustelulain suunnitelmista: Uhat siirtyneet tietoverkkoihin. Viitattu 7.4.2018. https://www.karjalainen.fi/uutiset/uutis-alueet/kotimaa/item/139551-tiedustelulain-suunnitelmat-julki-viranomaisten-valtuudet-kasvamassa-verkko-ja-ulkomaantiedusteluun

Knape, P. 2017. Siviilitiedustelulainsäädäntö - Muutokset poliisin valtuuksissa. Viitattu 26.3.2018. http://teknologiateollisuus.fi/sites/default/files/file_attachments/siviilitiedustelu_knape.pdf

Keskisuomalainen. 2016. Kanerva: Brysselin iskut osoittavat tiedustelulain muutoksen tarpeellisuuden. Viitattu 27.3.2018. https://www.ksml.fi/kotimaa/Kanerva-Brysselin-iskut-osoittavat-tiedustelulain-muutoksen-tarpeellisuuden/748570

Limnéll, J. 2014. Kyberturvallisuus tarvitsee johtajuutta ja tekoja. Viitattu 3.4.2018. http://www.aaltopro.fi/blog/kyberturvallisuus-tarvitsee-johtajuutta-ja-tekoja.

Meriniemi, M. 2017. Laput pois silmiltä - nykymaailmassa tiedustelulaeille on kipeä tarve. Viitattu 7.4.2018. http://intermin.fi/ajankohtaista/blogi/-/blogs/laput-pois-silmilta-nykymaailmassa-tiedustelulaeille-on-kipea-tarve

Puolustusministeriö. 2015c. Parlamentaarinen seurantaryhmä tiedustelulainsäädännön uudistamiseen liittyville hankkeille. Viitattu 19.3.2018. https://www.defmin.fi/ajankohtaista/tiedotteet/2015/parlamentaarinen_seurantaryhma_tiedustelulainsaadannon_uudistamiseen_liittyville_hankkeille.7565.news

Savon Sanomat. 2018. Viattomuuden aika on ohi sosiaalisessa mediassa. Viitattu 6.4.2018. https://www.savonsanomat.fi/paakirjoitukset/Viattomuuden-aika-on-ohi-sosiaalisessa-mediassa/1127424

Sisäministeriö 2017. Suomi tarvitsee siviilitiedustelua kansallisen turvallisuuden suojaamiseen. Viitattu 27.3.2018. http://intermin.fi/artikkeli/-/asset_publisher/suomi-tarvitsee-siviilitiedustelua-kansallisen-turvallisuuden-suojaamiseen

Sisäministeriö. 2018. Siviilitiedustelulainsäädännön valmistelu. Viitattu 19.3.2018. http://intermin.fi/tiedustelu

Suomen yrittäjät. 2018. Yrittäjyys Suomessa. Viitattu 7.4.2018. https://www.yrittajat.fi/suomen-yrittajat/yrittajyys-suomessa-316363

Susi, M. 2017. Elinkeinoelämän näkökulmia tiedustelulainsäädäntöön. Viitattu 29.4.2018. https://teknologiateollisuus.fi/sites/default/files/file_attachments/elinkeinoelaman_nakokulmia_susi.pdf

Tekniikka & talous. 2017. Elinkeinoelämän kelkka kääntyi täysin: tiedustelulait eivät haittaa bisnestä - Ruotsin malli onkin hyvä. Viitattu 26.3.2018. https://www.tekniikkatalous.fi/ttpaiva/elinkeinoelaman-kelkka-kaantyi-taysin-tiedustelulait-eivat-haittaa-bisnesta-ruotsin-malli-onkin-hyva-6642716

Tekniikka & talous. 2017b. Kyberturvallisuus synnyttää 20 000 uutta työpaikkaa muutamassa vuodessa - Osaajapula voi tappaa nousun Pohjoismaiden ykköseksi. Viitattu 6.4.2018. https://www.tekniikkatalous.fi/tekniikka/ict/kyberturvallisuus-synnyttaa-20-000-uutta-tyopaikkaa-muutamassa-vuodessa-osaajapula-voi-tappaa-nousun-pohjoismaiden-ykkoseksi-6681177

Tietosuojavaltuuten toimisto. 2018. EU:n tietosuojauudistus. Viitattu 28.4.2018. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html

Tietoviikko. 2014. HS: Tällä ohjelmalla varastettiin rekkalasteittain tietoja Suomen ulkoministeriöstä. Viitattu 15.2.2018. https://www.tivi.fi/Uutiset/2014-09-26/HS-T%C3%A4ll%C3%A4-ohjelmalla-varastettiin-rekkalasteittain-tietoja-Suomen-ulkoministeri%C3%B6st%C3%A4-3148941.html

Tietoviikko. 2018. Gdpr on kohta täällä, rikkoja voi saada jopa 20 miljoonan sakot - näin organisaatiot valmistautuvat asetukseen. Viitattu 18.3.2018. https://www.tivi.fi/Kaikki_uutiset/gdpr-on-taalla-kohta-rikkoja-voi-saada-jopa-20-miljoonan-sakot-nain-organisaatiot-valmistautuvat-asetukseen-6701121

Tilastokeskus. 2014. Digitalisaatio yritysten liiketoiminnassa 2012-2014. Viitattu 2.4.2018. http://www.stat.fi/til/inn/2014/inn_2014_2016-06-02_kat_007_fi.html

Varsinais-Suomen yrittäjät. 2017. EU:n tietosuoja-asetus koskee kaikkia yrityksiä - Aloita valmistautuminen viimeistään nyt. Viitattu 29.3.2018. https://www.yrittajat.fi/varsinais-suomen-yrittajat/a/uutiset/564916-eun-tietosuoja-asetus-koskee-kaikkia-yrityksia-aloita-valmistautuminen-viimeistaan

Verkkouutiset. 2018. Näin perustuslakia halutaan muuttaa tiedustelulakien takia. Viitattu 28.3.2018. https://www.verkkouutiset.fi/nain-perustuslakia-halutaan-muuttaa-tiedustelulakien-takia/

Verkkouutiset. 2018b. Vihreiden mukaan turvallisuuden lisäksi on puolustettava vapauksia ja oikeuksia. Viitattu 6.4.2018. https://www.verkkouutiset.fi/vihreiden-mukaan-turvallisuuden-lisaksi-on-puolustettava-vapauksia-ja-oikeuksia/

Viestintävirasto. 2017. HAVARO havainnoi ja varoittaa tietoturvaloukkauksista. Viitattu 3.4.2018. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/05/ttn201605241520.html

Yleisradio. 2014. Supo: Ulkoministeriö joutui kaksi kertaa vakoilun kohteeksi. Viitattu 28.4.2018. https://yle.fi/uutiset/3-7332824

Yleisradio. 2017. Tiedustelulakien säätämiskiire puhuttaa Turun iskun jälkeen - Näin kansalaisten viestintää valvotaan Saksassa, Ranskassa ja Ruotsissa. Viitattu 20.2.2018. https://yle.fi/uutiset/3-9794972

Yleisradio. 2017b. Kiisteltyyn tiedustelulakiin tulossa tiukennuksia - Yle sai salaiset lakipykälät etukäteen nähtäväksi. Viitattu 6.4.2018. https://yle.fi/uutiset/3-9967517

Yleisradio 2018. Analyysi: Oppositio kiusaa hallitusta tiedustelulailla. Viitattu 19.3.2018. https://yle.fi/uutiset/3-10041634

Virallislähteet

HaVL 7/2018 vp. Hallintovaliokunnan lausunto perustusvaliokunnalle.

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

Puolustusministeriö. 2015. Suomalaisen tiedustelulainsäädännön suuntaviivoja - lausuntoyhteenveto tiedonhankintalakityöryhmän mietinnöstä. 30.6.2015.

Puolustusministeriö. 2015b. Suomalaisen tiedustelulainsäädännön suuntaviivoja - tiedonhankintalakityöryhmän mietintö. 14.1.2015.

Sisäministeriö. 2015. Asettamispäätös 1.10.2015, diaari SMDno-2015-1509.

Sisäministeriön julkaisu 8/2017. 2017. Siviilitiedustelulainsäädäntö - siviilitiedustelulakityöryhmän mietintö.

Sisäministeriön julkaisu 16/2017. 2017. Siviilitiedustelun ja suojelupoliisin ohjauksen kehittäminen sisäministeriön hallinnonalalla - työryhmän raportti.

Sisäministeriön julkaisu 21/2017. 2017. Siviilitiedustelu - lausuntotiivistelmä.

Turvallisuuskomitea. 2013. Suomen kyberturvallisuusstrategia. Helsinki: Puolustusministeriö.

Turvallisuuskomitea. 2017. Yhteiskunnan turvallisuusstrategia. Helsinki: Turvallisuuskomitea.

Valtioneuvoston kanslia. 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017.

Viestintävirasto. 2014. Kyberturvallisuuskeskus - toimintasuunnitelma.

Liite 1: Haastattelurunko

LAUREA AMMATTIKORKEAKOULU | Yhdessä enemmän |

Haastattelu 1

x.x.2017

Haastattelu - Etunimi Sukunimi, Organisaatio

Johdanto

Sisäministeriö asetti loppuvuodesta 2015 monialaisen työryhmän valmistelemaan ehdotusta uudeksi siviilitiedustelulakikokonaisuudeksi. Siviilitiedustelulakityöryhmä luovutti mietintönsä huhtikuussa 2017. Mietintö on lausuntokierroksella kesäkuuhun 2017 saakka. Lausuntokierroksen jälkeen tavoitteena on saada esitys eduskunnan käsittelyyn tulevalla syysistuntokaudella 2017.

Valmisteilla olevan siviililainsäädäntöhankkeen tarkoituksena on kehittää Suomen kykyä suojautua entistä paremmin kansalliseen turvallisuuteen kohdistuvilta vakavilta uhkilta, kuten esimerkiksi terrorismilta tai vieraiden valtioiden Suomeen kohdistamalta vakoilulta.

Sisäministeriön työryhmän mietinnössä ehdotetaan uuden siviilitiedustelua koskevan luvun lisäämistä poliisilakiin sekä kokonaan uutta lakia tietoliikennetiedustelusta siviilitiedustelussa. Mietinnön mukaan suojelupoliisilla tulisi olla toimivaltuudet ulkomaan henkilötiedusteluun ja tietojärjestelmätiedusteluun sekä tietoliikennetiedusteluun.

Tietoliikennetiedustelu tarkoittaisi Suomen rajan viestintäverkossa ylittävään tietoliikenteeseen, osin automaattisesti, kohdistuvaa tiedonhankintaa sekä tällä tavoin hankitun tiedon käsittelyä. Tietojärjestelmätiedustelulla tarkoitetaan ulkomaisessa tietojärjestelmässä käsiteltäviin tietoihin kohdistuvaa tietoteknisin keinoin tapahtuvaa tiedustelua.

Kyseinen opinnäytetyö käsittelee siviilitiedustelulakihanketta erityisesti tietoliikennetiedustelun ja tietojärjestelmätiedustelun näkökulmasta. Työn tarkoituksena on selvittää millaisia vaikutuksia kyseisillä menetelmillä voisi olla erityisesti tietointensiivisten (esim. tuotekehitys) yritysten toimintaan.

Laurea-ammattikorkeakoulu
Ratatie 22, 01300 Vantaa
Puhelin (09) 8868 7150
Faksi (09) 8868 7200
etunimi.sukunimi@laurea.fi
www.laurea.fi
Y-tunnus 1046216-1
Kotipaikka Vantaa

LAUREA AMMATTIKORKEAKOULU | Yhdessä enemmän |

Haastattelu 2

x.x.2017

Haastattelukysymykset

1. Voitko kertoa millaisia työtehtäviä sinulla on XXX-organisaatiossa?
2. Onko XXX-organisaatiolla toimintaa kyberturvallisuuden ja tietoturvan alueella?
3. Oletko tutustunut käynnissä olevaan siviilitiedustelulainsäädäntöhankkeeseen?
4. Onko XXX-organisaatio ollut mukana lakihankkeen valmistelussa esimerkiksi antamassa lausuntoja?
5. Miten arvioisit suomalaisten yritysten ja organisaatioiden kyberturvallisuuden tasoa tällä hetkellä? Mitä vahvuuksia tai puutteita siinä on?
6. Onko valmisteilla olevalle siviilitiedustelulainsäädännölle tarvetta?
7. Näetkö tiedustelulakihankkeessa jotain puutteita tai haittoja yritysten liiketoiminnalle?
8. Millaisia vaikutuksia esimerkiksi tietoverkkotiedustelulla voisi olla yrityksille ja organisaatioille?
9. Tulisiko yritysten ja organisaatioiden olla mukana tiedustelulain toteuttamisessa (esim. tietoverkkotiedustelun käytännön toteutus tai rahoitus)?
10. Miten arvioisit elinkeinoelämän, yritysten sekä organisaatioiden huomioimista siviilitiedustelulainsäädäntöhankkeen aikana?
11. Tietoverkkotiedustelulain tarkoituksena olisi muun muassa hankkia tietoja ulkomaisesta tiedustelutoiminnasta. Yritysvakoilusta on saatukin viitteitä myös Suomessa (Case Ulkoministeriö). Vaikuttaako lakihanke organisaatioiden toimintaedellytyksiin ja tiedon suojaamiseen?
12. Miten arvioisit siviilitiedustelulakihankkeen mahdollisia vaikutuksia yritysten investointihalukkuuteen tulevaisuudessa?

Laurea-ammattikorkeakoulu
Ratatie 22, 01300 Vantaa
Puhelin (09) 8868 7150
Faksi (09) 8868 7200
etunimi.sukunimi@laurea.fi
www.laurea.fi
Y-tunnus 1046216-1
Kotipaikka Vantaa

13. Siviilitiedustelulakityöryhmän mietinnön mukaan toimintaa valvottaisiin sekä parlamentaarisesti että viranomaisvoimin. Esimerkkinä viranomaisvalvonnasta toimintaa valvomaan perustettaisiin erillinen ja puolueeton tiedusteluvaltuutettu, jolla olisi laajat toimivaltuudet ja tiedonsaantioikeudet. Miten arvioisit valmistelua tehneen työryhmän ehdotuksia tiedustelutoiminnan valvonnasta?

14. Millaisia kyvykkyyksiä yritykset ja organisaatiot tarvitsevat tulevaisuudessa kyberturvallisuuden ja esimerkiksi tietoliikennetiedustelun näkökulmasta?

15. Millaisia vaikutuksia lainsäädäntöhankkeella voisi olla yritysten ja organisaatioiden luottamukseen teknologiasta ja yksityisyydensuojasta?

16. Voiko valmisteilla olevalla siviilitiedustelulainsäädäntöhankkeella olla vaikutuksia Suomen maineelle korkean tietosuojan tai tietoturvan maana?