Finnish Information Security Cluster (FISC) – Kyberala ry

Lausunto

09.01.2026

Asia: VN/10644/2024

# Lausuntopyyntö luonnoksesta hallituksen esitykseksi sotilastiedustelusta annetun lain muuttamisesta ja siihen liittyviksi laeiksi

## Lausunnonantajan lausunto

**Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään**

Teknologiateollisuus, sekä Kyberala kiittävät mahdollisuudesta lausua asiasta (yhteinen lausunto). Teknologiateollisuus ry edustaa yli 1800 jäsenyritystä, jotka vastaavat puolesta Suomen viennistä, tutkimus- ja kehitysinvestoinneista ja työllistävät suoraan ja välillisesti neljäsosan suomalaisista. Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyberturvallisuusalaa.

Teknologiateollisuus ry ja Kyberala ry pitävät sotilastiedustelulainsäädännön päivittämistä perusteltuna muuttuneen turvallisuusympäristön vuoksi, mutta katsovat, että esitetyt muutokset tarkastelevat kokonaisuutta osin liian kapeasti. Korostamme taloudellisten vaikutusten, yritysten toimintaedellytysten, EU-oikeuden ja perusoikeuksien suojan laajempaa huomiointia sekä tarvetta tarkentaa toimivaltuuksien rajoja, valvontaa ja vaikutusarvioita. Ehdotuksia tuetaan siltä osin kuin ne parantavat tarkoituksenmukaista, kohdennettua ja oikeusvaltioperiaatteiden mukaista tiedustelutoimintaa, mutta useisiin kohtiin esitetään täsmennyksiä ja varauksia, jotta sääntely tukisi sekä kansallista turvallisuutta että elinkeinoelämän ja yritystalouden toimivuutta.

Tiivistelmä

Ehdotuksella on hyväksyttävä tavoite kehittää sotilastiedustelulainsäädäntöä muuttuneen turvallisuusympäristön ja voimassa olevan lain soveltamisesta kertyneiden havaintojen mukaisesti. Ehdotus on kuitenkin osin perusteltu kapeasti, eikä ota riittävästi huomioon muuttuneen toimintaympäristön, teknologian kehityksen tai hallitusohjelman tavoitteiden kokonaisuutta ja lakiehdotuksen vaikutuksia yrityksiin ja talouteen. Erityisen merkityksellistä on, mitä etua laajemmista ja perusoikeuksien ydinalueelle osin entistä pidemmälle ulottuvilla toimivaltuuksilla on yhteiskunnalle laajemmin ja sen toimijoille, kuten kansalaisille ja yrityksille. Kun

tiedusteluvaltuuksien käyttö ulottuisi myös näihin ryhmiin, valtiokeskeisiä perusteita tulisi laajentaa vastaavasti. Yhdymme ehdotuksessa esitettyyn kantaan, että sotilastiedusteluviranomaisen toiminnan tulee olla lainalaista, tarkoituksenmukaista, tehokasta ja ajantasaista. Yhteenvetona toteamme, että:

1. Sotilastiedustelun kehittämisessä tulisi arvioida taloudelliset vaikutukset laajemmin, myös hallitusohjelman tavoitteiden osalta, koska vahva talous on myös turvallisuuden edellytys.

2. Tietojärjestelmätiedustelun (kotimaa) laajentaminen loogisesti määriteltyihin järjestelmäkokonaisuuksiin on kannatettava.

3. Tietoliikennetiedustelun hakuehtouudistus on kannatettava, mutta ilmoitusvelvollisuudesta ei tule luopua ilman poikkeussääntöä: ilmoitus tulisi jatkossakin tehdä Suomessa laillisesti oleskelevalle henkilölle, laillisesti toimivalle yritykselle tai yhteisölle, kun toimenpiteen tarkoitus on lakannut, ellei ennakoitavissa ole merkittävää haittaa valtion yleiselle edulle. Tuomioistuimen tulisi antaa lupa ilmoittamatta jättämiselle.

4. Viestinnän välittäjien avustamisvelvollisuus on kannatettava ehdotus, ja valtion on korvattava kaikki siitä aiheutuvat välittömät kustannukset, mukaan lukien työvoimakulut.

5. Ehdotettu muutos 104 §:ään on perusteltu, mutta tulisi varmistua, ettei tietojen saanti poikkea muualla säädettyjen salaisten tiedonhankintakeinojen välttämättömyysedellytyksestä sekä eritoten tuomioistuinlupaa koskevasta vaatimuksesta, eikä johda yleiseen päästä-päähän salauksen heikentymiseen Suomessa.

6. Peitetoimivaltuuden rajat ja valvonta tulisi kirjata tarkasti lakiin, ja toimivallan käyttö tulisi rajata soveltuvalla tavalla Pääesikunnan sotilastiedusteluviranomaiselle.

7. Sivullisten laitteisiin kohdistuvan toimivallan vaikutusarvio ja perustelut ovat osin puutteellisia: yritysten aineeton omaisuus ja mainehaitat tulisi huomioida, ja lisäksi tulisi välttää tahattomasti vaikutelman syntymistä sotilastiedusteluvirkahenkilöiden taloudellisten etujen edistämisestä tavalla, joka on ristiriidassa virassa hankittujen salassa pidettävien tietojen hyväksikäyttökiellon kanssa.

8. Ulkomaisiin tietojärjestelmiin kohdistuvat estotoimet sisältävät merkittäviä ulko- ja turvallisuuspoliittisia riskejä; päätökset tulisi tehdä poliittisella tasolla ja aina poikkihallinnollisesti valmistellen sekä vain välittömästi uhkaavan sotilaallisen uhkan torjumiseksi.

Yhdymme lisäksi Elinkeinoelämän keskusliitto EK:n lausuntoon sekä Puolustus- ja ilmailuteollisuus PIA ry:n lausunnon yhteenvedon kohtiin 1, 4 sekä 6 niiltä osin, kuin ne kuuluvat nyt ehdotetun lainsäädännön alaan. Kohdan 3 osalta olennaista on, että nyt käsillä olevassa lakiehdotuksessa huomioidaan soveltuvin osin VN/1886/2025 hallituksen esitys laiksi sähköisen viestinnän palveluista annetun lain muuttamisesta (radiohäirintään tarkoitetut laitteet) liittyvät vaikutukset.

Orpon hallitusohjelman lähtökohdat

Lakiehdotuksessa perustellaan sotilastiedustelulainsäädännön kehittämistä Orpon hallitusohjelman puolustusta ja turvallisuutta koskevista kirjauksista. Ehdotuksessa ei kuitenkaan huomioida riittävästi koko hallitusohjelman toimintaperiaatteita (s. 7–8), jotka muodostavat kaikkia kirjauksia ohjaavat, ja osin rajoittavatkin, reunaehdot eri toimenpiteiden toteuttamiselle.

Toimintaperiaatteiden mukaan Suomen vahva demokratia ja korkea luottamus julkisiin instituutioihin rakentuvat avoimesta, vastuullisesta ja johdonmukaisesta hallinnosta, joka edistää turvallisuutta, yhdenvertaisuutta, osaamista ja hyvinvointia sekä toimii osana sääntöpohjaista kansainvälistä järjestelmää. Hallitus vaalii oikeusvaltiota ja huolellista, tietoperustaista lainvalmistelua varmistaakseen yhteiskunnan vakauden ja perusoikeuksien suojan. Kansalaisten ja viranomaisten välisessä suhteessa vaalitaan hyvän hallinnon periaatteita. Muita periaatteita ovat:

- Hyvinvoinnin perusta on kestävä talous ja tärkein talouspoliittinen tavoite on kestävä kasvu
- Avoimeen markkinatalouteen perustuvan oikeusvaltion rooli on toimivan, turvallisen ja oikeudenmukaisen yhteiskunnan rakentaminen
- Poliittisen- ja hallintovallan tehtävä on tarjota puitteet vapaudelle ja mahdollisuuksille

Ehdotuksessa on käsitelty kattavasti Orpon hallitusohjelman tavoitteita tiedustelulainsäädännön kehittämisestä viranomaisten toimintakyvyn turvaamiseksi osana kansallisen puolustuskyvyn ja turvallisuuden kokonaisuutta. Koska kestävä (ts. vahva) talous on myös yhteiskunnan kriisinsietokyvyn, kansallisen puolustuskyvyn ja sisäisen turvallisuuden ylläpitämisen tärkein strateginen edellytys, tulisi varmistaa, että ehdotetut sotilastiedustelun kehittämiseen tai toimivaltuuksien laajentamiseen liittyvät toimet eivät vaaranna tai heikennä tämän tavoitteen saavuttamista. Ehdotuksen vaikutukset elinkeinoelämään, yrityksiin ja talouteen tulisi siten käsitellä kattavammin jatkovalmistelussa. Myös oikeussubjektien vapauden varmistaminen edellyttää, että valtio ei puutu lailliseen toimintaan enempää, kuin on välttämätöntä. Muiden yllä mainittujen reunaehtojen osalta huomiot löytyvät kustakin keskeistä muutosehdotusta koskevasta osiosta alta.

Suhtaudumme varauksellisesti sotilastiedustelulainsäädännön muutostarpeiden laajamittaista perustelua Suomen NATO-jäsenyydellä, eritoten niiltä osin, joissa voi syntyä vaikutelma, että Suomella olisi velvoite toteuttaa lainsäädännöllisiä sotilastiedustelujärjestelmän yhteensopivuustoimia. Mikäli tällaisia on, tulisi ne eritellä lakiehdotuksessa. Peruste, jonka mukaan ”monet NATO-maat ovat antaneet laajempia toimivaltuuksia omille puolustushallinnoilleen” ei välttämättä tavoita suomalaisen yhteiskunnan kokonaisetua. Korostamme, että Suomen tulee itsenäisesti harkita itselleen soveltuvimmat menettelyt ja toimivaltuudet, sillä jäsenyys puolustusliitossa ei käsityksemme mukaan edellytä kansallisten suorituskykyjen tai toimivaltuuksien yhdenmukaistamista tai ”erinomaisuutta” suhteessa muihin liittokunnan jäseniin, vaikka toki liittokunnan yhteiset tarpeet on tarpeen ottaa huomioon. Suomella on omat vahvuutensa puolustusasioissa ja sen tulee kyetä myös valitsemaan ja priorisoimaan itselleen tarkoituksenmukaisimmat ratkaisut.

Kotimaassa tapahtuva valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu

Ehdotuksessa säädettäisiin uudesta tietojärjestelmätiedustelun toimivaltuudesta, jonka avulla voitaisiin hankkia tietoteknisin menetelmin tietoa sotilaallisesta tai kansallista turvallisuutta vakavasti uhkaavaan toimintaan hyödynnettävän tietojärjestelmän toiminnasta, sen sisältämistä tiedoista, tietojärjestelmän osien välillä liikkuvista viesteistä sekä tietojärjestelmään saapuvista tai siitä lähtevistä viesteistä. Keskeistä on, että tuomioistuimen lupa ei rajautuisi yksittäiseen laitteeseen (kuten nykyinen tekninen laitetarkkailu), vaan loogisesti määriteltyyn järjestelmäkokonaisuuteen. Tämä vastaa paremmin modernia, hajautettua tieto- ja viestintäjärjestelmiä koskevaa toimintaympäristöä ja on siten kannatettava. On kuitenkin tarpeen, että ”loogisesti” määritelty järjestelmäkokonaisuus käsitellään siten, että tuomioistuimen on mahdollista yksiselitteisesti ymmärtää ja valvoa, millaiseen tietojärjestelmäkokonaisuuteen ja kenen hallintaoikeuden piiriin toiminta kohdistuu. Tähän liittyvät edellytykset tulisi kuvata mahdollisimman tarkkaan säädöstasolla ja lain esitöissä.

Tietoliikennetiedustelu

Ehdotuksessa säädettäisiin uudesta toimivaltuudesta, hakuehtojen määrittämisestä. Hakuehtojen määrittämisessä pyritään tunnistamaan tietoliikennevirrasta kohteeseen liittyviä säännönmukaisuuksia ja ominaispiirteitä, joita voidaan käyttää varsinaisen tietoliikennetiedustelun hakuehtoina. Toimivaltuuksista poistettaisiin kielto käyttää viestin sisältöön meneviä hakuehtoja sekä kielto käyttää Suomessa olevaa tai oletettavasti olevaa telepäätelaitetta tai -osoitetta hakuehtona.

Pidämme muutosta kannatettavana, sillä hakuehtojen määrittäminen ja sisällöllisten hakuehtojen kiellon poistamisen voidaan arvioida osittain parantavan yksityisyyden suojaa tietoliikennetiedustelun tarkemman kohdentumisen myötä ja tehostavan tietoliikennetiedustelun tehokkuutta. Kuitenkin, koska kyseessä on tällöin viestinnän sisältöön kohdistuva valvonta, ilmoittamisesta luopumisen osalta tulisi huomioida alla asiaa koskevassa osiossa todettu.

Myös uusi toimivaltuus, joka mahdollistaa satunnaisen tietoliikenteen otannan hakuehtojen kehittämistä varten sekä otantatiedon säilyttämisen 12 kuukaudeksi, on kannatettava. Muutoksen voidaan arvioida parantavan hakuehtojen tarkkuutta siten, että ne osuvat todennäköisemmin uhkatoimintaan eivätkä sivullisiin.

Tietoliikennetiedustelun ilmoittamisesta luopuminen

Ehdotuksen mukaan muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta ilmoittamisesta luovuttaisiin. Käsityksemme mukaan perusteet ilmoitusvelvollisuudesta luopumiseen ovat ymmärrettäviä. Lähtökohtaisesti kuitenkin Suomessa laillisesti oleskelevalla henkilöllä tai laillisesti toimivalla yrityksellä tai yhteisöllä on oikeus tietää, mikäli hän on joutunut viranomaisen toimenpiteen kohteeksi. Tätä tietoa on pidettävä oikeusturvan lähtökohtana. Vaikka

kolmannet osapuolet, muut viranomaiset ja julkiset instituutiot valvoisivatkin oikeuksien toteutumista toimenpiteiden kohteeksi joutuneen puolesta, tätä ei voine pitää täysin verrannollisena oikeusturvan takeena. Ehdotuksessa todetaankin, että viranomaisen ei tarvitse tosiasiassa käsitellä tietoja, jotta kyse olisi yksityiselämään puuttumisesta, vaan puuttumiseksi on katsottava jo se, että viranomainen kerää ja tallentaa niitä myöhempää käyttöä varten (EIT: Marper v. Yhdistynyt Kuningaskunta). Edelleen lainauksena ”EIT on ratkaisuissaan toistuvasti korostanut sitä, että yksityiselämän suojaan puuttuvan, salaiset viranomaistoimenpiteet mahdollistavan lain on oltava oikeusvaltioperiaatteiden mukainen, kansalaisten saatavilla sekä laadultaan sellainen, että kansalaiset kykenevät ennakoimaan sen soveltamisen seuraukset omalta osaltaan.”

Luottamuksen säilyttämiseksi oikeusvaltioperiaatteen noudattamiseen sekä Suomeen tietoyhteiskuntana erityisesti tietoliikennetiedustelun osalta tulisi huolehtia siitä, että sen kohteeksi joutunut Suomessa laillisesti oleskeleva henkilö, laillisesti toimiva yritys tai yhteisö saa tiedon salaisen viranomaistoimenpiteen kohteeksi joutumisesta, kun toimenpiteen tarkoitus on lakannut. Ilmoitusta ei kuitenkaan olisi välttämätöntä tehdä, mikäli ilmoitus vaarantaisi toimenpiteen tarkoituksen tai jos on ennakoitavissa merkittävää haittaa valtion yleiselle edulle. Tuomioistuimen tulisi aina päättää ilmoituksesta luopumisesta.

Viestinnän välittäjän ja tietoyhteiskunnan palvelun tarjoajan avustamisvelvollisuus ja tietojen saanti

Pidämme ehdotuksen mukaisesti kannatettavana, että tiedonsiirtäjällä (esim. teleoperaattori tai muu viestinnän välittäjä) olisi velvollisuus myötävaikuttaa tietoliikennetiedustelun liityntäpisteen toteuttamiseen ja ylläpitämiseen, antaa Puolustusvoimien tiedustelulaitokselle tarvittavat tekniset tiedot, antaa pääsy tiloihin, joissa liityntäpiste rakennetaan. Käytännössä muita viestinnän välittäjiä ovat esim. datakeskustoimijat. Poikkeuksena ehdotetaan oikeutta toteuttaa liityntäpiste ilman tiedonsiirtäjän myötävaikutusta, mikäli tiedonsiirtäjän kanssa toteutus ei onnistu, tai se on välttämätöntä sotilastiedustelun suojaamiseksi. Tällöinkin tiedonsiirtäjän tulee olla paikalla, mikäli tämä on mahdollista ilman, että tiedustelutoiminnan suoja vaarantuu. Lisäksi tiedonsiirtäjällä ja tietoyhteiskunnan palveluntarjoajalla olisi oikeus saada valtion varoista korvaus liityntäpisteen toteuttamisesta aiheutuneista välittömistä kustannuksista. Ehdotusta voidaan pitää perusteltuna huomioiden tele- ja datakeskusmarkkinan kehityssuunta sekä toimijoiden kasvava monimuotoisuus Suomessa.

Ehdotettujen muutosten ei tule aiheuttaa tilannetta, että ko. palveluita tarjoavat yritykset tai yhteisöt joutuisivat luopumaan päästä-päähän salauksesta (E2EE), helpottamaan tai mahdollistamaan sotilastiedusteluviranomaisten pääsyä järjestelmiinsä tai palveluihinsa yleisesti. Menettely vaarantaisi kaupallisten toimijoiden välistä välttämätöntä luottamuspääomaa, oikeutta yksityiseen viestintään sekä yritysvarallisuuden arvon säilyttämistä ja elinkeinotoiminnan taloudellisten edellytyksistä huolehtimista. Lisäksi menettely heikentäisi Suomen kokonaisturvallisuuden tavoitteita. Valtioneuvosto, sekä myös Puolustusministeriö on aiemmissa asiaan liittyvissä lainvalmisteluissa ylläpitänyt selvää kantaa päästä-päähän salauksen välttämättömyydestä Suomen kokonaisturvallisuudelle.

Koska säädösehdotus lisäsi tosiasiassa viranomaisten toimivaltuuksia tehdä myös omavaltaisesti ja salaisesti yritysten ja yhteisöjen hallintaoikeuden piiriin kuuluvassa viestintäinfrastruktuurissa (verkossa) toimenpiteitä, jotka voivat aiheuttaa myös toiminta- ja kyberturvallisuushäiriöitä eli vahinkoriskin. Katsomme, että jatkovalmistelussa ainakin liityntäpisteen toteuttamisen osalta ehdotukseen sisällytetään täsmällisemmät menettely-, vastuu- ja korvaussäännökset.

Lakiehdotus jättää epäselväksi, johtaako ehdotetun 99 §:n ja 100 §:n (jota ei ehdoteta muutettavaksi) kokonaisuus epäyhdenvertaiseen tilanteeseen. 99 §:n mukaan viestinnän välittäjällä ja tietoyhteiskunnan palvelun tarjoajalla on oikeus saada korvaus SVPL 299 §:n mukaan (henkilöstökuluja ei korvata), mutta 100 §:n mukaan tiedonsiirtäjällä on oikeus saada valtion varoista korvaus 97 §:n (sotilastiedusteluviranomaisen avustaminen) ja 98 §:n (tietojen antaminen) aiheutuneista välittömistä kustannuksista, jotka voivat käsityksemme mukaan sisältää myös välittömiä henkilöstökustannuksia. Lakiehdotuksessa tulisi varmistaa, että menettely on yhdenvertainen ja työvoiman käytöstä syntyneet välittömät kustannukset sisältyvät korvaukseen.

Tietojen saantioikeutta (104 §) koskien ehdotuksessa todetaan, että pykälän 2 momenttia muutettaisiin vastaamaan sitä, mitä muualla esimerkiksi rikostorjunnan osalta säädetään. Lisäksi todetaan, että salaisten tiedonhankintakeinojen säännöksiä tulisi uudistaa yhdenmukaisesti ja että sääntely on mahdollisimman samansisältöistä. Ehdotettua muutosta voidaan pitää perusteltuna. Käsityksemme mukaan kuitenkin 2 momentti mahdollistaisi pyytämään tietoja (välitys-, tunnistamis- ja mahdollisesti muut tiedustelutehtävän kannalta tarpeelliset tiedot), joiden hankkimiseen muualla lainsäädännössä (mm. Pakkokeinolain 10 luku, salaiset pakkokeinot sekä Poliisilaki 5 luku, salaiset tiedonhankintakeinot) edellytettäisiin tuomioistuimen lupaa. Lisäksi edellytyksenä salaisten pakko- ja tiedonhankintakeinojen käytölle on, että hankittavilla tiedoilla on erittäin tärkeä merkitys tehtävän suorittamiselle. Arviomme mukaan muutosehdotus voi olla tahattomasti ristiriidassa edellä viitattujen sääntelytavoitteiden kanssa. Katsomme, että säännöksen osalta tulisikin varmistua, että se on linjassa muualla laissa olevien salaisten pakko- ja tiedonhankintakeinojen käytön edellytysten kanssa.

Kiinnitämme tietojensaanti- ja avustusvelvoitteisiin liittyen erityistä huomiota myös siihen, että Valtioneuvosto on käynnistänyt (5.12.2025) datakeskusten rekisteröintivelvollisuutta ja rekisterin perustamista koskevan poikkihallinnollisen lainsäädäntöhankkeen. Rekisteröintivelvoite tuottaisi viranomaisille nykyistä paremman ja kokonaisvaltaisemman tilannekuvan datakeskustoimijoista ja toiminnasta. EU:n datakeskustietokannan ja voimassa olevin Kyberturvallisuuslain (124/2025) kanssa päällekkäinen tiedonkeruu datakeskustoimijoilta tai tietoyhteiskunnan toimijoilta ylipäätään tulisi rajoittaa vain tietoon, jota ei ole jo muutoin saatavissa. Rekisteröitymisvelvoitteen toteuttaminen ja tarkoituksenmukaisuus tulisi varmistaa erityisesti yhteissijoitusdatakeskusten tai yhteisisännöintidatakeskusten (EU 2024/1364 Art. 2, kohdat 2 ja 3) tapauksissa, missä datakeskuksen ylläpitäjä ja käyttäjät ovat eri juridisia toimijoita. Rekisteröintivelvoitteeseen liittyviä kaavailuja mahdollisista vastuuviranomaisista rekisterin toimeenpanoon voisivat olla esimerkiksi Energiavirasto, joka jo koordinoi tietojen keruuta EU:n datakeskustietokantaan tai Liikenne- ja viestintävirasto Traficom siinä tapauksessa, mikäli rekisteröintivelvollisuus toteutettaisiin sähköisen viestinnän palvelulaissa olevia ilmoitusvelvoitteita (Osa II, 2. Luku 4 §) täydentämällä koskemaan datakeskuksia.

Tiedonhankinta yleisesti saatavilla olevista lähteistä

Puolustusvoimista annettuun lakiin lisättäisiin säännökset tiedonhankinnasta yleisesti saatavilla olevista lähteistä. Tietoa voitaisiin hankkia automaattisesti ja manuaalisesti. Liityntä Puolustusvoimiin voitaisiin peittää käyttämällä vääriä, harhauttavia tai peiteltyjä tietoja. Suomessa ei ole ollut aiemmin sääntelyä, jolla olisi varmistettu, että toiminta on kaikilta osin lainalaisuusperiaatteen alaista. Ehdotukseen sisältyisi myös oikeus käyttää ns. ”peitettä” eli oikeutta mm. rekisteröityä palveluihin tekaistuilla, harhauttavilla tai peitellyillä tiedoilla, jotta tiedonhankinnan alkuperää ei paljasteta. Tältä osin kyseessä olisi poikkeus viranomaistoiminnan julkisuutta koskevaan periaatteeseen sekä siihen, että Suomessa laillisesti toimivalla yrityksellä tai yhteisöllä on oikeus tietää, mikäli hän on joutunut viranomaisen toimenpiteen kohteeksi. Kun otetaan huomioon, että lakiehdotuksessa ehdotetaan myös puolustushaarojen määrittämistä tietyiltä osin sotilastiedusteluviranomaisiksi, sääntelyn ei tulisi johtaa tilanteeseen, jossa viranomainen laajamittaisesti pyrkisi käyttämään tekaistuja, harhauttavia tai peiteltyjä tietoa laillisissa palveluissa. On tärkeää huomata, että laillisesti toimivilla palveluntarjoajilla on oikeus asettaa käyttöehtoja palveluilleen ja lienee oletusarvoisesti selvää, että ko. toimivaltuuden käyttö olisi useimmiten käyttöehtojen vastaista. Toiminta voisi johtaa epätarkoituksenmukaisiin tilanteisiin sekä aiheuttaa yrityksille tarpeettomia kustannuksia. Lisäksi olisi huomioitava, että toimintaa ohjaavan sisäisen määräyksen sisältö olisi todennäköisesti myös salassa pidettävä, joten toimintaa ei olisi mahdollista valvoa muutoin, kuin esim. sisäisen tai tiedusteluvaltuutetun valvonnan avulla. Näin ollen on perusteltua, että säännöstasolle kirjattaisiin toiminnan rajat sekä valvontamenettelyt aiempaa tarkemmin ja/tai rajata kyseisen toimivaltuuden käyttö, tai ainakin ohjaus- ja valvontavastuu Pääesikunnan sotilastiedusteluviranomaiselle.

Laitteen, menetelmän tai ohjelmiston asennus ja poisottaminen

Lakiehdotuksen mukaan sotilastiedustelu voisi käyttää myös sivullisten laitteita tai tietojärjestelmiä, jos se olisi välttämätöntä menetelmän tai ohjelmiston asentamiseksi tai poisottamiseksi. Yksittäisen toimenpiteen ei arvioida puuttuvan merkittävästi omaisuuden suojaan, sillä toimenpiteen keston voidaan katsoa olevan varsin vähäinen. Ehdotamme, että asiaa koskevaan säännökseen (Laki sotilastiedustelusta, 42 §, 2 mom.) lisätään maininta oikeushenkilöstä sekä kustannusten korvaamisesta: ”Sotilastiedusteluviranomaisen pyynnöstä viranomaisen ulkopuolisella luonnollisella tai oikeushenkilöllä on oikeus tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen ohjauksessa ja valvonnassa toteuttaa tiedustelumenetelmän käytön edellyttämä asennus- tai poistamistoimenpide. Tiedusteluviranomaisen on korvattava toimenpiteestä aiheutuvat kustannukset.”

Ehdotuksen perusoikeusvaikutusten arvioinnissa esille nostettu omaisuuden suojaan liittyvä arvio on käsityksemme mukaan puutteellinen.  Suomella on merkittävää potentiaalia digi-, datateollisuudessa ja -taloudessa ja Suomen on viennistä riippuvainen talous. Vaikka tarkkojen laskelmien tuottaminen voi olla vaikeaa, on tarpeen arvioida myös vaikutuksia toimenpiteen kohteelle aineettoman omaisuuden sekä liiketaloudelliseen toimintaan erottamattomasti kuuluvan luottamuksen osalta, kun kohteena on yritys tai yhteisö, jonka tuoteisiin tai palveluihin toimivallan käyttö kohdistuu. Tästä

näkökulmasta toimenpiteen kestolla tai ylipäätään käyttäjälle ilmenevällä vähäisellä palvelun saatavuushäiriöllä ei ole olennaista merkitystä asiassa, vaan sillä, mitä seurauksia toimivallan käytöstä on niille toimijoille, joiden omistamiin tai hallitsemiin tuotteisiin tai palveluihin toiminta kohdistuu. Vaikutusarvioinnin tulisi huomioida näkökulma, että yrityssalaisuuksien sekä muun liiketoimintaa koskevan tiedon luottamuksellisuus on yritysten elinehto ja luottamus toimijoihin on taloudellista arvoa sisältävää mainepääomaa. Tästä näkökulmasta on merkitystä sillä, kuinka laajaa toimivallan käyttäminen olisi, miten laillisesti toimivat yritykset ja yhteisöt voisivat pienentää luottamuksellisuuteen liittyviä riskejään sekä milloin toimenpiteen kohteeksi joutumisesta ilmoitetaan (ks. yllä kohta ”Tietoliikennetiedustelun ilmoittamisesta luopuminen”). Toimenpiteiden toteuttamisen ei tulisi johtaa tilanteeseen, jossa Suomessa laillisesti toimivan yrityksen tai yhteisön kyberturvallisuuden taso muutoin heikentyisi toimivaltuuksien käytön seurauksena.

Ehdotuksen perusoikeusvaikutusten arvioinnissa todetaan myös, että muutoksella olisi myönteisiä vaikutuksia sotilasviranomaisen palveluksesta eronneen virkamiehen oikeuteen työhön ja elinkeinovapauteen (PL 18 §) tilanteessa, jossa virkamies on saavuttanut puolustusvoimista annetun lain 47 §:n mukaisen eroamisiän ja hänellä omaa sotilastiedustelutoiminnassa tarpeellisia tietoja ja taitoja. Katsomme, että vaikkakin huomio eittämättä pitää paikkaansa, perustelu voidaan tulkita myös keinona edistää sotilastiedusteluvirkahenkilöiden omia taloudellisia intressejä luomalla markkinaolosuhteita, joissa sotilastiedusteluun virkasuhteessa aiemmin olleet pyrkisivät vastikeperustaiseen tai liiketoiminnalliseen monopoliasemaan. Lisäksi lienee kiistatonta, että ko. tiedot – myös taidot niiltä osin, kun on kyse esimerkiksi salaista tiedonhankintaa, taktisia toimintamalleja tai operatiivista toimintaa koskevista tiedoista – kuuluvat lain mukaan hyväksikäyttökiellon piiriin. Viranomaisen palveluksessa toimiva (myös entinen virkamies, harjoittelija tai avustaja) ei saa paljastaa tai käyttää virassa hankittua salassa pidettävää tietoa omaksi tai kenenkään muun hyväksi tai vahingoksi.

Suomen ulkopuolella olevan tietojärjestelmän käytön estäminen tai sen toiminnan haittaaminen vakavan vaaran torjumiseksi

Esitysluonnoksessa ehdotetaan uutta toimivaltuutta, jonka avulla sotilastiedusteluviranomainen voisi estää ulkomailla sijaitsevan tietojärjestelmän käytön, haitata tai muokata sen toimintaa edellyttäen, että kyseinen järjestelmä voi aiheuttaa Suomen maanpuolustukselle tai kansalliselle turvallisuudelle vakavaa vaaraa. Perusteluna esitetään, että kyberuhat, disinformaatio ja hybridivaikuttaminen tapahtuvat usein valtioiden rajojen ulkopuolelta, että joissakin tilanteissa uhkaa ei voida estää diplomatialla, rikostutkinnalla tai pakotteilla.

Vaikka ehdotetussa sääntelyssä ei ole kyse aseelliseen voimankäyttöön rinnastettavasta toiminnasta, toimenpiteellä voi olla sen luonteen mukaan ulko- ja turvallisuuspoliittisia vaikutuksia. Käsityksemme mukaan ehdotetulle toimivallalle ei ole olemassa kansainvälisen oikeuden mukaista oikeusperustaa (muutoin kuin YK:n peruskirjan 51 artiklan tarkoittamassa itsepuolustus aseellisen hyökkäyksen tilanteessa) riippumatta siitä, onko toimenpide sallittu kansallisen oikeuden mukaisesti. Tällöin toimenpiteen kohdevaltiolla olisi edelleen syy vastatoimiin. Näin ollen ehdotetuilla

muutoksilla Suomen rajan ulkopuolella olevan tietojärjestelmän toimintaan vaikuttamisesta olisi vaikutuksia Suomen kansainvälisiin suhteisiin sekä myös Suomessa toimiviin yrityksiin.

Esimerkiksi Venäjän hybridioperaatioista vuosina 2022–2024 (EU, UK ja Yhdysvallat) merkittävä osa ja näistä on kohdistunut yrityksiin (kuljetus-, valmistava teollisuus-, ilmailu-, tietoliikenne-, energia-, terveydenhuoltoalat (lääkejakelu ja lääkinnälliset laitteet), vesihuolto sekä puolustusteollisuus). Lisäksi presidentti Niinistö toteaa valmousunionia koskevassa erityisraportissaan (Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness – Report by Sauli Niinistö, former President of the Republic of Finland In his capacity as Special Adviser to the President of the European Commission), että ”sabotaasi-iskut ja kyberhyökkäykset voivat häiritä talouden, energian, liikenteen ja digitaalisten verkkojen toimintaa – ja niiden vaikutukset voivat levitä myös muihin sektoreihin ja pahimmillaan vaarantaa ihmishenkiä. Haitalliset kybertoimet ovat lisääntyneet viime vuosina merkittävästi, ja ne näyttävät suurelta osin liittyvän geopoliittisiin jännitteisiin.” Suomessa presidentti Niinistön mainitsemat sektorit infrastruktuureineen ja palveluineen ovat pääosin yritysten hallussa.

Lisäksi lakiehdotuksessa, kuten sen taustalla olevissa selonteoissakin on todettu, että Venäjä on osoittanut, ettei se kunnioita toisten valtioiden suvereniteettia ja alueellista koskemattomuutta ja on toimillaan loukannut YK:n peruskirjaa sekä rikkonut eurooppalaista sopimuspohjaista turvallisuusjärjestystä. Koska Suomen ulkopuolella olevan tietojärjestelmän vahingoittaminen voidaan niin Venäjän, kuin monen muunkin mm. autoritäärisiä piirteitä omaavan valtion toimesta tulkita Suomen toteuttamaksi ”aggressioksi”, tai ainakin Suomeen kohdistuvia vastatoimia kiihdyttäväksi. Katsomme, että säännöksen lisääminen sotilastiedustelulakiin harkitaan hyvin tarkkaan. Mikäli toimivalta annettaisiin, tulisi säännöksissä asettaa selkeät ja yksiselitteiset takeet, miten ja missä tilanteissa sotatilan tai poikkeusolojen ulkopuolella on toimivaltaisen viranomaisen sallittua pyrkiä tilanteeseen, jossa se voisi toteuttaa ko. toimenpiteen (operaation). Pidämme todennäköisenä, että mikäli esitettyä toimivaltuutta käytettäisiin, kielteisiä seurannaisvaikutuksia (mahdollisten myönteisten seurausten lisäksi) syntyisi erityisesti Suomessa toimiville yrityksille. Seuraukset voisivat olla tietoturvallisuushäiriöitä, liiketoiminta- ja toimitusketjuihin kohdistuvia häiriöitä tai muutoin kauppaan kohdistuvia kielteisiä seurauksia.

Lisäksi erikseen tilanteissa, joissa ei ole kyse välittömästä sotilaallisesta Suomen kansallista turvallisuutta vakavasti vaarantavan toiminnan estämisestä tai haittaamisesta, sotilastiedusteluun liittyviä toimivaltuuksien käyttö tulisi rajoittaa ainoastaan virka-apuun liittyen muun viranomaisen tehtävän tukemiseksi yleisen järjestyksen ja turvallisuuden ylläpitämiseksi, terrorismirikosten ja muiden ihmisten hengelle tai terveydelle vakavaa vaaraa aiheuttavien rikosten estämiseksi ja keskeyttämiseksi. Tähän liittyvät mahdolliset tehtävä- ja toimivaltakysymykset tulisi käsitellä muita viranomaisia koskevassa lainsäädännössä.

Katsomme, että päätös toimivallan käytöstä tulisi aina tehdä poliittisella tasolla, esimerkiksi Tasavallan Presidentin tai soveltuvan ministeriryhmän toimesta sen lisäksi, mitä ehdotuksessa sanotaan erikseen merkittäviä ulkopoliittisia vaikutuksia ja suhteita vieraisiin valtioihin koskevien riskien vaikutuksista. Koska on oletettavaa, että seurannaisvaikutukset voivat olla moninaisia, on välttämätöntä, että harkittavan toimenpiteiden seurannaisvaikutukset käsitellään ja arvioidaan hallinnonalat ylittävällä menettelyllä. Ko. asia tulisikin aina valmistella poikkihallinnollisesti, ja

saattaa esimerkiksi tasavallan presidentin ja ulko- ja turvallisuuspoliittisen ministerivaliokunnan (TP-UTVA) käsiteltäväksi.

Sund Peter
Finnish Information Security Cluster (FISC) – Kyberala ry - Teknlologiateollisuus ry (yhteinen lausunto)