7.4.2015

**Puolustusministeriölle**

# CSC – Tieteen tietotekniikan keskus Oy:n lausunto Tiedonhankintalakityöryhmän mietintöön (FI.PLM.2015-218; 909/40.02.00/2013)

CSC – Tieteen tietotekniikan keskus Oy (jäljempänä CSC) kiittää mahdollisuudesta lausua Tiedonhankintalakityöryhmän mietinnöstä ”Suomalaisen tiedustelulainsäädännön suuntaviivoja”. Kyseisessä mietinnössä esitetyistä kehitysehdotuksista erityisesti tietoliikennetiedusteluun liittyvillä ehdotuksilla on vaikutusta CSC:n toimintaan. Näin ollen tässä lausunnossa keskitytään tietoliikennetiedustelua käsitteleviin ehdotuksiin.

## Johdanto

Tietoverkkoturvallisuus on tänä päivänä yhä keskeisempi osa kansallista turvallisuutta, ja varautuminen kyberuhkiin on tärkeä elementti yhteiskunnan elintärkeiden toimintojen turvaamisessa. Viranomaisilla on oltava mahdollisimman selkeät toimivaltuudet, ja tarvitaan laajapohjaista yhteistyötä viranomaisten, yritysten ja kaikkien muiden kriittistä infrastruktuuria hallussaan pitävien toimijoiden kesken. Verkottuneessa ja digitalisoituneessa maailmassa on yhä selvempää, että tehokas turvallisuusuhkien torjuminen vaatii riittäviä keinoja valtioiden rajat ylittävien verkkoa hyödyntävien uhkien torjumiseen. Tiedonhankinnassa tulee pyrkiä riittävään läpinäkyvyyteen, jossa selvästi rajataan tiedonhankintamenetelmät ja selkiytetään valtuudet.

Vaikka tietoverkot tuovat mukanaan uudenlaisia uhkia, digitalisaatio ja verkottuminen tuovat mukanaan myös huomattavia myönteisiä vaikutuksia ja uusia mahdollisuuksia taloudelle ja kilpailukyvylle. Digitalisaatiota pidetäänkin avaintekijänä Suomen talouskasvun edistämisessä, ja sen myönteisiä vaikutuksia ei tule arvioida erillään tietoverkkoturvallisuuden näkökulmasta tehdystä viranomaisten toimivaltuuksien arvioinnista. Teknisesti muuttuvassa toimintaympäristössä tarvitaan käytössä olevien keinojen arviointia siitä näkökulmasta, mikä on tehokasta. Suomen kilpailukyvyn kannalta on lisäksi tärkeää varmistaa, että käytetään sellaisia tiedonhankintakeinoja, joilla ei vaaranneta yritysten tietojen luottamuksellisuutta ja kansalaisten tai asiakkaiden tietosuojaa esimerkiksi tietovuotojen kautta.

Verkkomaailmassa tapahtuneet nopeat muutokset, kuten pilvipalveluiden ja teollisen internetin nousu yhä merkittävämpään asemaan, voivat muuttaa toimintaympäristöä myös siitä näkökulmasta, minkälaisilla keinoilla tiedustelua on hyödyllistä harjoittaa. Tänä päivänä on vaikea määritellä, mikä on kansallisten rajojen sisäistä ja mikä niiden ylittävää tietoliikennettä. Ei ole näin ollen itsestään selvää, että esimerkiksi tietoverkkovalvonnan keinoilla päästään enää tulevaisuudessa käsiksi kaikkeen turvallisuuden kannalta relevanttiin tietoliikenteeseen, vaan voidaan joutua pohtimaan uudenlaisia keinoja. Toisaalta ei voida myöskään taata, että esimerkiksi tietoliikennetiedustelu ei kohdistuisi Suomen sisäiseen tietoliikenteeseen, koska Suomen sisäinenkään tietoliikenne ei välttämättä kulje pelkästään Suomen rajojen sisällä. Siksi on välttämätöntä, että tietoverkkoturvallisuutta pohditaan kokonaisvaltaisesti ja arvioidaan lainsäädäntötarpeita mahdollisimman laajassa viitekehyksessä siten, että esimerkiksi tiedonhankintalakityöryhmän mietinnössä esitettyjen uusien viranomaistoimivaltuuksien kustannukset ja vaikutukset sekä kansalliseen turvallisuuteen että talouteen ja kilpailukykyyn arvioitaan huolellisesti. Asian jatkotyöstämiselle on tärkeää muodostaa riittävän laaja pohja ja yhteistyöfoorumi, jossa käytävä avoin dialogi edistää niin kansallista turvallisuutta kuin kilpailukykyäkin. Tässä keskustelussa tulee olla mukana elinkeinoelämän ja keskeisten verkko- ja infrastruktuuritoimijoiden edustus. Myös riittävä tekninen asiantuntemus on oltava edustettuna.

## Tiedonhankintalainsäädännön jatkovalmistelussa huomioitavia seikkoja

Tiedonhankintalakityöryhmän mietintö herättää joitakin kysymyksiä, joihin CSC pitää erityisen tärkeänä kiinnittää huomiota jatkovalmistelussa:

## 1. Teknisen osaamisen ja ratkaisujen hyödyntämisen arviointi

Olisiko verkkouhkiin mahdollista varautua nykyisen lainsäädännön puitteissa kehittämällä teknisiä ratkaisuja? Kyberympäristön suojelu on pitkälti tekninen kysymys, johon Suomesta löytyy osaamista. Tekninen kehitys tuo lisäksi omat haasteensa tiedonhankinnalle verkkotiedustelun keinoin mm. salaustekniikoiden yleistymisen, käyttötapojen muuttumisen ja verkon käyttäjämäärien kasvaessa. Tietoliikenteen datamäärien arvioidaan kolminkertaistuvan vuoteen 2017 mennessä. Tekniseltä kannalta tilanne muuttuu tietoverkkotiedustelun kannalta jatkuvasti huonompaan suuntaan. Vanhan sähköpostityyppisen A:sta B:hen viestinnän tilalla ovat paljolti pilvipalvelut (A-C, B-C), jolloin viestinnän tosiasialliset päätepisteet eivät enää paljastu yksittäisestä viestistä. Tämä korostaa entisestään tarvetta kartoittaa kattavasti tietoverkkotiedustelun hyödyt ja vaikutukset kokonaisvaltaisesti. Suomessa olevaa teknistä osaamista tulisi hyödyntää ja tähän liittyvien keskeisten tahojen tulisi olla mukana jatkovalmistelussa. Salaustekniikoiden kehittyminen on myös kustannuskysymys: tulee selvittää, minkälaisia taloudellisia resursseja mahdollinen salausten purkaminen vaatii. Salauksen yleistymisen vuoksi verkkoliikenteen tiedustelun arvo itse asiassa saattaa laskea hyvinkin nopeasti. Koska lähes kaikki merkittävät viestintäpalvelut ja sosiaaliset mediat toimivat Suomen ulkopuolella, ei myöskään sitä kautta ole pääsyä viestiliikenteeseen. On siis mahdollista, että vuosia sitten muissa maissa tehtyjen ratkaisujen toistaminen ainoastaan tuhoaa merkittävän ja kipeästi kaivatun kilpailutekijän suomalaiselta IT-teollisuudelta, sekä heikentää kansalaisten luottamusta viranomaisiin. Siksi kansainvälisten kokemusten tarkka arviointi on ehdottomasti tehtävä ennen päätöksiä. Erilaisten tiedonhankintakeinojen tehokkuutta ja vaikutuksia Suomen kansalliseen turvallisuuteen tulisi arvioida kattavasti eri näkökulmat huomioiden, jotta voidaan muodostaa riittävän kattava näkemys lainsäädännöllisistä tarpeista. Näitä vaikutuksia tulee punnita suhteessa erilaisista keinoista aiheutuviin kustannuksiin ja kansantaloudellisiin vaikutuksiin ottaen huomioon myös tekniset realiteetit. Mietinnössä todetaan, että tiedon hankinta ei sinällään vielä olisi keino estää uhkien toteutumista, ja että rajapinta tiedustelun ja torjuntatoimien välillä tulisi järjestää erikseen. CSC on samaa mieltä mietinnön linjauksen kanssa, jonka mukaan jatkovalmistelussa on tärkeää selvittää ja arvioida tiedustelun ja uhkien torjunnan yhteyttä paitsi lainsäädännön ja viranomaistoimivaltuuksien, myös teknisen toteutuksen näkökulmasta. Näin ollen teknisten asiantuntijoiden ottaminen mukaan jatkotyöskentelyyn on välttämätöntä.

## 2. Tietoliikenteen olennaisten toimijoiden tunnistaminen ja kustannukset

Mikäli valmistellaan sellaista lainsäädäntöä, joka asettaa velvoitteita (esimerkiksi liityntäpisteiden osoittamista tietoliikennetiedusteluun liittyen) yrityksille ja muille tietoliikennetoimijoille, tulee huomioida tästä aiheutuvat investointi- ja ylläpitokulut. Erityisesti julkisten toimijoiden tietoliikennetoiminnan erityispiirteet tulee ottaa huomioon, ja valtion tulee kattaa kaikki näistä velvoitteista aiheutuvat kustannukset vähintäänkin julkisten toimijoiden osalta. Lisäksi on kiinnitettävä erityistä huomiota tietoliikennetoimijoiden verkoissa kulkevan tietoliikenteen luottamuksellisuuteen. Erityisiä teknisiä vaatimuksia ja kustannuksia tietoliikenteen osalta tulee olemaan niiden toimijoiden osalta, joiden verkoissa on sensitiivistä dataa, kuten terveystietoa. Keskeiset tietoliikennetoimijat tulee ottaa mukaan jatkovalmisteluun.

## 3. Suomen kilpailukyvyn näkökulma

Meneillään oleva tietoliikenneyhteyksien kehittäminen ja sitä kautta Suomen kehittäminen turvallisena ja nopeana tietoliikenteen läpikulkupaikkana vahvistaa osaltaan Suomen asemaa houkuttelevana maana datakeskusinvestoinneille ja on keskeinen tekijä Suomen tulevaisuuden kannalta. Tietoliikenneyhteyksien kehittäminen on tärkeää digitalouden hyödyntämisen, uuden teollisuuden ja liiketoiminnan syntymisen kannalta. Pilvipalveluiden arvioidaan kasvavan noin 40 prosentin vuosivauhtia. Erityisesti big datan hyödyntämistä ajatellen on tärkeää, että verkot toimivat hyvin ja turvallisesti, sekä kansallisesti että globaalisti. Suurten datamäärien varastointi ja käsittely edellyttävät mahdollisimman tehokasta datakeskustoimintaa. Jotta voidaan varmistaa uuden dataintensiivisen liiketoiminnan sijoittuminen Suomeen, on tärkeää jatkuvasti kehittää verkkoinfrastruktuuriamme ja pitää edistää Suomen houkuttelevuutta luotettavana ja turvallisena tietoliikenteen kauttakulkumaana sekä houkuttelevana paikkana datakeskusinvestoinneille. Tietoverkkoja hyödyntävän rikollisuuden torjuminen on tärkeä osa tietoverkkojen turvallisuutta ja luotettavuutta. Tätä tulee tarkastella objektiivisesti sekä erilaisista tiedonhankintavaltuuksista aiheutuvien vaikutusten, niin hyötyjen kuin haittojenkin näkökulmasta. Mahdolliset haitat, jotka voivat liittyvä esimerkiksi verkoissa tapahtuvan viestinnän luottamuksellisuuden vaarantumiseen ja sen seurauksiin niin yksilöille, yrityksille kuin koko yhteiskunnalle, tulee selvittää ja arvioida kun edetään lainsäädännön valmistelutyössä. Tiedonhankintalainsäädännön jatkotyössä tulee huomioida kansallisen kilpailukyvyn ja innovaatiotoiminnan näkökulmat ja ottaa näiden sektoreiden asiantuntijoita mukaan työhön.

## Yhteenveto

CSC katsoo, että Tiedonhankintalakityöryhmän mietintö (mukaan lukien liitteet sekä LVM:n ja TEMin esittämät eriävät mielipiteet) nostaa yhteiskunnalliseen keskusteluun merkittävän asian. Muuttuneessa toimintaympäristössä tulee huolehtia siitä, että valtion ylin johto saa oikea-aikaista, oleellista tietoa, ja että viranomaisilla on selkeät toimivaltuudet. CSC:n näkemyksen mukaan Tiedonhankintalakityöryhmän mietintö ei kuitenkaan muodosta riittävää tietopohjaa lainsäädännön valmistelulle, eikä siinä ole tarpeeksi kattavasti huomioitu tietoliikennetiedustelun vaikutuksia yhteiskunnalle ja kilpailukyvylle. Näiden vaikutusten huomioiminen jatkovalmistelussa on välttämätöntä. Lisäksi CSC katsoo, ettei mietinnön valmistelu ole tapahtunut riittävän laajalla pohjalla. Elinkeinoelämän ja keskeisten tietoliikennetoimijoiden sekä teknisen asiantuntemuksen tulee olla edustettuna jatkovalmistelussa. Tavoitteena tulee olla mahdollisimman laaja ja kokonaisvaltainen eri toimijoiden yhteinen näkemys siitä, mitkä ovat tehokkaimmat tiedonhankinnan keinot Suomeen kohdistuviin tietoverkkoja hyödyntäviin uhkiin varautumiseksi. Tässä työssä tulee huomioida useita seikkoja, kuten maamme kilpailukyky, tekniset reunaehdot, kustannukset ja digitalisaation kehitys sekä sen mukanaan tuomat uudet mahdollisuudet.

Espoossa, 7.4.2015

CSC – Tieteen tietotekniikan keskus Oy

Kimmo Koski, toimitusjohtaja

*CSC – Tieteen tietotekniikan keskus Oy (CSC) tarjoaa tutkimuksen, opetuksen, kulttuurin ja hallinnon tarpeisiin tietoteknisiä palveluita ja resursseja. Tutkijat voivat käyttää Suomen laajinta tieteellisten ohjelmistojen ja tieteen tietokantojen valikoimaa sekä Suomen tehokkaimpia supertietokoneita Funet-tietoliikenneyhteyksien kautta. CSC on valtio-omisteinen, opetus- ja kulttuuriministeriön hallinnoima voittoa tavoittelematon yhtiö.*