Tietoliikenteen ja tietotekniikan keskusliitto,
FiCom ry
Lintulahdenkatu 10
00500 Helsinki

10.4.2015

Puolustusministeriö
kirjaamo@defmin.fi

Viite Suomalaisen tiedustelulainsäädännön suuntaviivoja
Tiedonhankintalakityöryhmän mietintö; lausuntopyyntö, 9.2.2015
FI.PLM.2015-218; 909/40.02.00/2013

FiComin lausunto suomalaisen tiedustelulainsäädännön suuntaviivoja selvittäneen työryhmän mietinnöstä

Puolustusministeriö asetti vuoden 2013 lopulla työryhmän kehittämään lainsäädäntöä turvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi kybertoimintaympäristön uhkista. Työryhmä luovutti mietintönsä kuluvan vuoden tammikuussa.

Puolustusministeriö on pyytänyt Tietoliikenteen ja tietotekniikan keskusliitto, FiCom ry:ltä lausuntoa työryhmän mietinnöstä, jossa arvioidaan tiedustelua koskevan lainsäädännön kehittämistarpeita.

Ministeriö on pyytänyt erityisesti näkemyksiä mietintöön sisältyvistä kehittämisehdotuksista ja johtopäätöksistä (mietinnön luvut 6 ja 7) sekä ehdotusten vaikutuksista lausunnon antajan toimintaan tai toimialalla.

FiCom kiittää mahdollisuudesta saada lausua asiassa ja esittää lausuntonaan seuraavaa:

Mietinnön parhaana puolena voitaneen pitää sitä, että siinä on tarkasteltu tehtävänantoon liittyviä asioita hyvinkin avoimesti ottaen huomioon aiheen arkaluontoisuus. Mietinnössä on myös pyritty käsittelemään elinkeinoelämän tärkeinä pitämiä asioita avoimesti ja kattavasti.

FiComin keskeiset viestit:

- Jatkovalmistelu tulee vaiheistaa selvästi: ensin tiedustelua koskevan yleisen lain valmistelu ja sitten muut tarpeelliset muutokset
- Jatkovalmisteluun tulee kytkeä mukaan myös elinkeinoelämän edustus
- Päätösten on perustuttava faktoihin eikä fiktioihin
- Verkkotiedustelu ei välttämättä tule täyttämään mietinnössä esitetyssä muodossa siihen kohdistettuja odotuksia ja toiveita
- Vääränlaiset ratkaisut saattavat aiheuttaa suuria ja pitkäkestoisia vahinkoja

Lausunnon sisältö

1 Elinkeinopoliittiset peruskivet - Tiedustelulainsäädännön vaikutuksista elinkeinoelämään

FiCom pitää ehdottoman tärkeänä, että tiedustelulainsäädäntöä jatkossa valmisteltaessa seuraavat periaatteet tulee sisällyttää jatkovalmistelun toimeksiantoon:

- Luottamuksen Suomeen ja suomalaisiin ICT-alan toimijoihin tulee säilyä eikä sitä saa vaarantaa
- Suomen kiinnostavuutta investointikohteena ei saa vaarantaa
- Salausavaimia ei vaadita toimitettavaksi viranomaisille eikä salauksen käyttömahdollisuuksia saa rajata
- Ei velvollisuutta asentaa takaportteja ohjelmistoihin
- Kustannukset tiedusteluorganisaatioiden kannettavaksi

2 Jatkovalmistelusta

FiComin näkemyksen mukaan jatkotyö tulisi selkeästi vaiheistaa.

Ensimmäisessä vaiheessa tulisi tiedustelutoimintaa koskevaa yleistä lainsäädäntöä valmistella mietinnössä esitetyllä tavalla. Tässä yhteydessä tulisi tietoliikennetiedustelun mahdollinen tarve selvittää yleisellä tasolla osana tiedustelukokonaisuutta.

Mikäli ensimmäisessä vaiheessa tehdyn tarvekartoituksen perusteella tietoliikennetiedustelu nähdään tarpeelliseksi, käynnistetään digitalisaation ja muun teknisen kehityksen huomioon ottavan, tietoliikennetiedustelua koskevan *erillislain valmistelu.*

Elinkeinoelämän edustus pitää kytkeä mukaan jo yleislain valmisteluun etenkin niiltä osin, kuin tiedustelun ajatellaan palvelevan elinkeinoelämän intressejä. Yritysten mukanaolon tärkeys korostuu etenkin mahdollisen tietoliikennetiedustelun toteutukseen liittyviä kysymyksiä käsiteltäessä.

3 Tietoliikennetiedustelu: ”Väärin sammutettu” - kohtaavatko tavoitteet ja esitetyt keinot?

Mietinnössä on ansiokkaasti kuvattu tiedustelutoiminnan tavoitteita. Voidaan kuitenkin perustellusti esittää kysymys: saavutetaanko asetetut tavoitteet mietinnön ehdottamalla tavalla? Tullaanko tavoitteet saavuttamaan mietinnössä kuvatun kaltaisen tietoliikennetiedustelun avulla?

FiCom haluaa kiinnittää jatkovalmistelijoiden huomiota kehityssuuntiin, joiden vaikutus suunniteltavaan tietoliikennetiedustelun tuloksellisuuteen on merkittävä:

- salauksen käytön lisääntyminen; katso esimerkiksi
  - OECD: Recommendation of The Council Concerning Guidelines for Cryptography Policy (27 March 1997)
  - OECD Recommendation Electronic Authentication and OECD Guidance for Electronic Authentication (June 2007)
  - suurten kansainvälisten toimijoiden viimeaikaiset toimet salauksen käytön lisäämiseksi (Google, Microsoft, Yahoo, Amazon, jne.)
- liikennemäärien eksponentiaalinen kasvu
- harhautus- ja etenkin peiteoperaatiotaitojen kehittyminen, jolloin verkoista saatavan tiedustelutiedon perusteella johtopäätösten tekeminen tulee suurella todennäköisyydellä johtamaan vääriin tulkintoihin

Mietinnössä kuvattu tietoliikennetiedustelun tekninen toteutus juontanee alkunsa Ruotsissa käytössä olevasta mallista. Onko toteutustapa kuitenkaan enää tarkoituksenmukainen tavoiteltavien tulosten kannalta?

Ruotsin malli on yli kymmenen vuoden takaa, minkä jälkeen moni asia muuttunut. Esimerkiksi tietoliikenneverkkojen liikennemäärät ovat kyseisen ajankohdan jälkeen moninkertaistuneet[1] eikä kasvu näytä hidastumisen merkkejä. Lisäksi televerkkojen perustana nykyisin oleva IP-teknologia on muuttunut käytännössä täysin hallitsevaksi tekniikaksi perinteisten piirikytkentäisten verkkojen tilalle.

Tietoliikennetiedustelua käyttävissäkin maissa on alkanut kuulua hajaääniä, joissa nykyisin käytössä olevat järjestelyt on asetettu kyseenalaisiksi[2].

Mikäli tietoliikennetiedustelu päätettäisiin ottaa Suomessa käyttöön, *FiCom esittää harkittavaksi, tuottaisiko jokin muu kuin mietinnössä esitetty tekninen ratkaisu tiedustelun kokonaistavoitteiden kannalta paremman lopputuloksen?*

Tietoliikennetiedustelun toteuttaminen

Mikäli jatkovalmistelun perusteella tietoliikennetiedustelu päätettäisiin ottaa käyttöön, luku 6.1.4 ei esitetyssä muodossa luo parasta vaihtoehtoa järjestelmän toteuttamiselle.

FiComin näkemyksen mukaan toteuttamissuunnittelu tulee tehdä yhteistyössä alan toimijoiden kanssa, jotta saavutettaisiin tavoitteiden kannalta mahdollisimman hyvä lopputulos.

[1] Viestintäviraston toimialakatsauksen 1/2015 mukaan kotimaan matkaviestinverkoissa siirretyn datan määrä on 620 kertaistunut verrattuna vuoden 2007 tasoon. Vaikka tietoliikennetiedustelua ei olisikaan tarkoitus kohdistaa kyseiseen liikenteeseen, esimerkki osoittaa osaltaan todeksi väitteet teleliikenteen merkittävästä kasvusta.

[2] Esimerkiksi http://www.tomsguide.com/us/rsa-nsa-spy-program-useless,news-18384.html; viitattu 1.4.2015

Mietinnössä esitetyt tekniset vaihtoehdot ja niihin liittyvät näkemykset perustuvat osittain jopa virheellisiin tulkintoihin ja oletuksiin tietoliikenneverkkojen toiminnasta (katso liite).

Mietinnön mukaan teknisestä toiminnasta yrityksille mahdollisesti aiheutuvat suorat kustannukset katettaisiin tietoliikennetiedustelua käyttävien tahojen toimesta. *FiCom kannattaa mietinnössä esitettyjä linjauksia - yritykset eivät saa joutua maksamaan tiedustelutoiminnasta aiheutuvia kuluja.* Yritykset eivät myöskään saa joutua kilpailluilla markkinoilla eriarvoiseen asemaan valtiovallan toimenpiteistä johtuen sen perusteella, liittyykö yrityksen palveluihin ja tuotteisiin yrityksen omassa hallussa olevia ulkomaanyhteyksiä niihin kohdistuvien tiedustelutoiminnan aiheuttamien kustannusten takia.

4 ”Sudenkuoppia”

Mietinnön suurimpana puutteena voitaneen pitää sitä, että se ei käytännöllisesti katsoen lainkaan käsittele tietoliikennetiedusteluun liittyviä epävarmuustekijöitä.

Pahimmillaan tämä saattaa johtaa tilanteeseen, jossa tietoliikennetiedustelua koskevat päätökset ja investoinnit tehdään liian puutteellisten tietojen varassa.

Erillisselvityksen puutteiden takia mietinnössä esitetyt johtopäätökset jäävät vaille perusteluja: ne voivat pitää paikkansa, tai voivat olla perättömiä. Päätöksiä ei pidä perustaa mietinnössä esitettyihin väitteisiin, jotka joko ovat vailla todellisuuspohjaa tai jotka edustavat pelkästään yksipuolisia tulkintoja laajemman kokonaiskuvan välttämiseksi. Tämän lausunnon liitteessä on käsitelty tarkemmin edellä viitattuja näkemyksiä.

FiCom pitää työryhmämietintöä hyvänä lähtökohtana tiedustelutoiminnan suuntaviivoista ja mahdollisista jatkotoimista päätettäessä. Päätöksiä tehtäessä tulee ottaa huomioon tässä lausunnossa esitetyt näkemykset etenkin niiltä osin, joissa mietinnön sisältö on osoitettu virheelliseksi tai muutoin asetettu kyseenalaiseksi.

FiCom haluaa esittää vakavan huolensa tietoliikennetiedustelua koskevan julkisen keskustelun synnyttämästä mielikuvasta, jonka mukaan turvallisuusviranomaiset huolehtisivat valtakunnan rajoilla Suomen suojaamisesta ja puolustamisesta kyberhyökkäyksiä vastaan. Tämä on väärä mielikuva, jonka ruokkiminen tulee heikentämään kansallista kyberturvallisuutta. FiCom korostaa, että *haitallisen tietoliikenteen estäminen tai rajoittaminen valtakunnan rajoilla on lähes mahdotonta.* Tiedustelun avulla pystytään parhaassa tapauksessa ainoastaan tunnistamaan haitallinen liikenne. ”Valtakunnallinen puolustaminen” kyberhyökkäyksiä vastaan ei onnistu, vaan suojauksen tietoverkkouhkia vastaan on perustuttava ”kohdepuolustukseen”. Turvallisuusviranomainen hoitaa rajalla -ajattelu vaarantaa yksittäisten kansalaisten ja organisaatioiden panostukset omien tietojärjestelmiensä suojaamiseksi.

5 Hallinnollisen järjestämisen suuntaviivoista (luku 6.1.5)

FiCom pitää yleisellä tasolla luvussa esitettyjä periaatteita oikeansuuntaisina.

FiComin näkemyksen mukaan toimeksiantajaviranomaisten määrän tulisi olla mahdollisimman pieni.

6 Oikeusturvan kannalta huomioon otettavista seikoista (luku 6.1.6)

FiCom pitää yleisellä tasolla luvussa esitettyjä periaatteita oikeansuuntaisina.

FiCom haluaa erityisesti korostaa järjestelmän läpinäkyvyyttä ja sen turvaamista jatkovalmistelussa. Digitalisaatioon liittyy merkittäviä kansantalouden kasvuun vaikuttavia odotuksia. Tiedusteluun - ja etenkin tietoliikennetiedusteluun - käytettyjen keinojen laajuudesta ja tuloksellisuudesta tulisi säätää mahdollisimman kattava raportointivelvollisuus, jonka tarkoituksena olisi säilyttää kansalaisten luottamus digitaalisiin palveluihin.

Edelliseen liittyen *FiCom haluaa kiinnittää jatkovalmistelijoiden huomiota* merkittävien internet-toimijoiden yhdessä laatimaan ehdotukseen *niistä periaatteista*, jotka pitäisi globaalisti ottaa käyttöön kansallisen turvallisuuden turvaamiseen tarkoitettuja viranomaisten toimivaltuuksia käytettäessä ja suunniteltaessa. Periaatteet löytyvät verkko-osoitteesta https://www.reformgovernmentsurveillance.com.

Mietinnön mukaan tietoliikennetiedusteluviranomainen luovuttaa tiedot toimeksiantajaviranomaiselle. Jatkovalmistelussa tulee ottaa kantaa myös siihen, kenellä ja millä perusteilla tiedustelun avulla kerätyt tiedot on mahdollista luovuttaa kansainvälisille yhteistyötahoille.

7 Ulkomaan tietojärjestelmätiedustelusta (luku 6.1.2)

FiCom haluaa kiinnittää jatkovalmistelijoiden huomiota ulkomaan tietojärjestelmätiedusteluun liittyvään merkittävään periaatteelliseen kysymykseen: voiko Suomi sallia omille viranomaisilleen sellaisen toiminnan, joka on Suomen ratifioimien kansainvälisten sopimusten perusteella kriminalisoitu ja jonka mukaiset teot on määritelty kansallisessa lainsäädännössä rangaistaviksi?

Lisäävätkö kyseisen kaltaiset ratkaisut kansalaisten ja yritysten luottamusta verkkoon ja sen palveluihin? Viranomaisten toimintamahdollisuuksien lisääminen mietinnössä esitetyllä tavalla saattaa johtaa esimerkiksi yritysten kannalta ristiriitaisiin tilanteisiin: yhtäältä asiakkaat saattavat edellyttää pitkälle meneviä toimia tietoliikenteen luottamuksellisuuden varmistamiseksi ja toisaalta samaan aikaan yritykset toimivat viranomaisten kanssa yhteistyössä samaisen luottamuksellisuuden murtamiseksi.

Oma lukunsa on sen arviointi, missä määrin kyseisen kaltaisen viranomaisten toimintaoikeuden tulkitaan antavan ulkomaisille viranomaisille vastaavan oikeuden tunkeutua suomalaisten toimijoiden tietojärjestelmiin tasapuolisuuden nimissä? Tulemmeko samalla maalittaneeksi suomalaiset toimijat hyökkäysten kohteiksi?

FiCom näkisi, varsinkin pitkällä aikajänteellä, parempana ratkaisuna sen, että kyseisen kaltaista toimintaa ei "hiljaisesti hyväksytä" mietinnössä kuvatulla tavalla, vaan kaikenlaisesta, tietojärjestelmän omistajan kannalta oikeudettomasta tunkeutumisesta pitäisi aktiivisesti ja kaikin keinoin pyrkiä eroon.

Suomi voisi ottaa johtavan roolin kansainvälisillä foorumeilla luotettavan digitalisaation airuena ja digitalisaatioon kiinteästi liittyvän tietojärjestelmien turvallisuuden edistämisessä. Suomen pitäisi olla aloitteellinen ja ehdottaa kansainvälisiä sopimuksia ja käytäntöjä, joiden perusteella vahvistettaisiin kansainvälisestikin laajasti hyväksyttyjä oikeushyviä myös digitaalisessa kybertoimintaympäristössä.

KARI WIRMAN
Kari Wirman
Johtaja, turvallisuus ja jatkuvuuden hallinta
Tietoliikenteen ja tietotekniikan keskusliitto, FiCom ry

Tietoliikenteen ja tietotekniikan keskusliitto,
FiCom ry
Lintulahdenkatu 10
00500 Helsinki

10.4.2015

Liite: Näkemyksiä mietinnön yksittäisistä kohdista

1 5.2 Organisaatioiden mahdollisuudet havainnoida niihin kohdistuvia tietoturvauhkia

Mietinnön mukaan "Tietoverkkojen käyttäjinä olevat yritykset, yhteisöt ja viranomaiset suojautuvat tietoverkkouhilta tietoturvan avulla. Toimintaoikeuksista tietoturvasta huolehtimiseksi säädetään tietoyhteiskuntakaaren 272 §:ssä. Säännös antaa yrityksille, yhteisöille ja viranomaisille työkaluja niihin kohdistuvien kybertekojen havaitsemiseksi ja torjumiseksi. Havainnointitoimenpiteet suoritetaan hajautetusti, jolloin niiden laatu ja taso vaihtelevat organisaatiokohtaisesti."

Teksti antaa puutteellisen kuvan organisaatioiden mahdollisuuksista, sillä tietoyhteiskuntakaaren 272 § on vain yksi tietoturvallisuutta koskeva säännös. Muualla laissa on lukuisia säännöksiä, jotka edellyttävät organisaatioilta tietoturvatoimia mukaan lukien tietoturvauhkien havaitseminen ja torjuminen.

Yleisen käytännön ja tulkinnan mukaan vaatimusten täyttämisestä syntyy organisaatioille myös oikeuksia, joita vaatimusten toteuttaminen edellyttää. Tekstin viittaama tietoverkkoturvallisuus on ainoastaan yksi tietoturvallisuuden toteuttamiseen liittyvästä osa-alueesta.

Tietoyhteiskuntakaaren viitattu pykälä koskee siis ainoastaan pientä, joskin tärkeää tekijää toiminnan tietoturvasta huolehdittaessa.

Edelleen mietinnön mukaan " Viestintävirasto ei ole eikä voi olla osapuolena tässä luottamuksellisessa yhteistyössä, HAVARO-järjestelmään ei voida luovuttaa niitä tunnisteita, joiden merkitys kansallisen turvallisuuden suojaamiseksi on suurin."

Mikäli tietoja haittaohjelmatunnisteista ei voida kertoa Viestintävirastolle saatikka tietoverkkouhkien torjunnasta käytännössä vastaaville tahoille eli kybertekojen kohteena oleville organisaatioille, tiedustelun tuottamilla tunnistetiedoilla ei ole mitään käytännön vaikuttavuutta etenkään yhteiskunnan kriittisen infrastruktuurin suojaamisessa. Tietoja ei myöskään voida hyödyntää "rajoilla tapahtuvassa puolustamisessa", sillä rajoilla havaitun haitallisen tietoliikenteen estämiseksi tai rajoittamiseksi ei ole mitään keinoja käytettävissä.

2 Luku 6.1.3 Kansallisen tietoliikennetiedustelun mahdollisia suuntaviivoja

Sivun 63 ylälaidan viidessä ensimmäisessä kappaleessa on lueteltu joukko asioita, joihin tietoliikenne tiedustelua tulisi voida käyttää.

Käyttötarkoitukset ovat esitetyssä muodossa perusteltuja.

Mietinnössä ei ole arvioitu oikeastaan lainkaan tietoliikennetiedusteluun liittyviä epävarmuustekijöitä. Tuottaisiko tietoliikennetiedustelu todella sellaisia tietoja, joiden avulla käyttötarkoituksiin liittyvät tavoitteet olisi mahdollista saavuttaa? Vaikka tarve ja tavoitteet olisivatkin hyväksyttävissä, onko järjestelmän rakentaminen siihen liittyvien epävarmuustekijöiden johdosta tarkoituksenmukaista rakentaa? Toteuttamiseen liittyviä päätöksiä tehtäessä olisi vähintäänkin arvioitava esimerkiksi järjestelmän toteuttamisen aiheuttamia kustannuksia, imagoriskejä, elinkeinopoliittisia riskejä sekä muita vastaavia asioita suhteessa järjestelmän toteuttamisen avulla tavoiteltaviin hyötyihin.

Sivun 64 ylälaidassa (ensimmäinen kappale) kuvataan sitä, miksi ja millä tavoin mahdollisesti [kyber]teon kohteena olevalle yritykselle voitaisiin ilmoittaa mahdollisista havainnoista.

Yhdeksi tietoliikennetiedustelun kohteeksi on kuvattu kriittiseen infrastruktuuriin kohdistuvien tekojen havaitseminen. Mainitut infrastruktuurit ovat lähes poikkeuksetta yritysten omistuksessa ja niiden ylläpitämiä.

Tiedustelun käytöllä ei ole mainitussa käyttötarkoituksessa mitään mieltä, mikäli havainnoista ei voida kertoa tekojen kohteelle - tiedustelulla saatu tieto on vailla merkitystä.

Sivun 64 ylälaidan toinen kappale sisältää lauseen, jonka mukaan "olisi tarpeen analysoida tietoliikennevirtoja tietoliikennetiedustelun selektiivisyyden varmistamiseksi ja teknologisen kehityksen seuraamiseksi".

Mitä tämä tarkoittaa käytännössä? Mietintö ei anna vastausta kysymykseen. Asia jäänee jatkovalmistelun varaan.

3 Luku 6.1.4 Tietoliikennetiedustelun toteuttaminen

Tunnistamistieto-käsitettä on käytetty mietinnössä sekavasti. Sillä saatetaan tarkoittaa kumotussa viestintämarkkinalaissa tarkoitettuja tietoliikenteen tunnistamistietoja (tietoyhteiskuntakaaren mukaisia viestin välitystietoja) tai kyseisellä käsitteellä voidaan tarkoittaa jotain tunnistettavaa merkkijonoa, jonka perusteella bittivirrasta voitaisiin poimia kyseisen tunnisteen sisältämä viesti jatkokäsittelyyn.

Mietinnän tekstin mukaan ” Tietoliikennetiedustelu rajoittaisi eri vaiheissaan eri laajuudessa luottamuksellisen viestin suojaa. Tietoliikennetiedustelun alkuvaiheessa hakuehtoja verrattaisiin kaikkiin niihin viesteihin, jotka liikkuvat kohteeksi valikoiduissa tietoliikennevirroissa. -- Tässä vaiheessa vertailu voisi perustua muun tietoliikenteen kuin haittaohjelmaliikenteen osalta tunnistamistietoihin.”

Mikäli tunnistamistiedolla tarkoitetaan viestin välitystietoa, tiedustelu kohdistettaisiin edellä olevan perusteella tilaajan tai käyttäjän käytössä olevaan IP-osoitteeseen tai muuhun vastaavaan tunnisteeseen, mikä olisi käytännössä sama

asia kuin rajat ylittävän, tietyn tilaajan tai käyttäjän liikenteen telekuuntelu. Tämä ei kuitenkaan liene ollut tarkoitus.

Luvun tekstin perusteella jää täysin auki, miten tietoliikennetiedustelu kohdistettaisiin tiettyyn liikenteeseen, vaikka luvussa on pyritty kuvaamaan juuri kyseistä asiaa.

4 Luku 6.1.7 Tietoliikennetiedustelun vaikutusarviointia

Luku sisältää suuren joukon väitteitä, joiden paikkansapitävyys on valitettavan helppo myös kiistää.

Elinkeinoelämän mahdollisuuksista suojautua tietoverkkouhkia vastaan

(Kohdan 6.1.7 neljäs kappale:) "Tietoliikennetiedustelu täydentäisi merkittävällä tavalla Suomen suojautumista vakavimpia tietoverkkouhkia vastaan. Nykyiset järjestelmät eivät havaitse valtiollisia vakoilu- ja muita haittaohjelmia, joiden kansallista turvallisuutta vahingoittava vaikutus on erityisen suuri. Tietoliikennetiedustelusta olisi hyötyä myös elinkeinoelämän suojautumisessa kaikkein vakavimpia tietoverkkouhkia vastaan."

Kova väite, jonka voidaan perustellusti väittää olevan perätön.

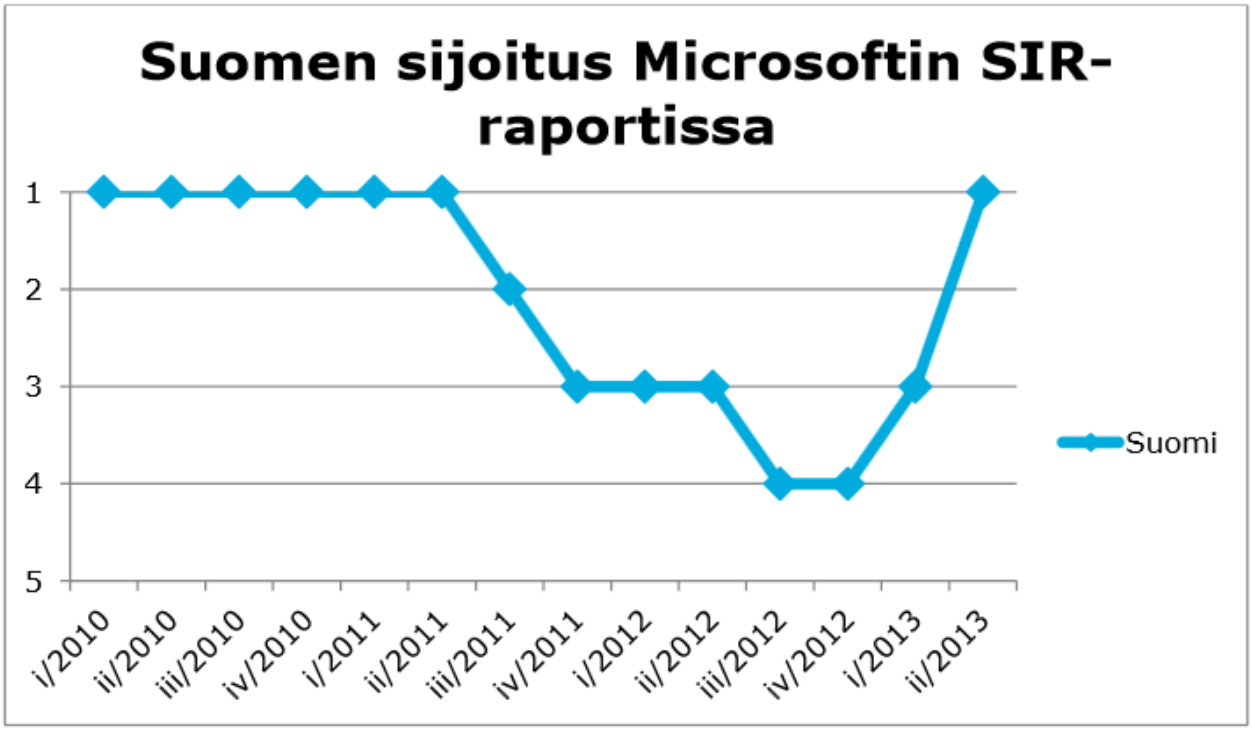
Tekstistä syntyvä mielikuva tietoliikennetiedustelun hyödyistä on vailla todellisuuspohjaa. Teksti antaa ymmärtää, että tiedustelu paikkaisi nykyiset haittaohjelmien havaitsemisessa olevat puutteet. Näin ei kuitenkaan käytännössä tulisi olemaan: tiedusteluyhteisön yhteistyön perusteella saatettaisiin saada havaitsemisen kannalta hyödyllistä lisätietoa, mutta missään tapauksessa kyseiset tiedot eivät voisi nekään olla 100 % täydellisiä. Haittaohjelmien toimintaperiaatteet muuttuvat jatkuvasti, joten tiedusteluyhteistyön kautta saadut tiedot nekin vanhenevat yhä nopeammin. Apu olisi parhaimmillaankin vain hetkellinen. Lisäksi on pidettävä mielessä, että suurin osa haittaohjelmista on suunnattu ”arkisempiin tarkoituksiin” kuin julkishallinnon toimintaa vastaan. Haittaohjelmia vastaan taistellaan jatkuvasti ja torjunta sekä torjunnan periaatteet muotoutuvat jokapäiväisten käytännön tarpeiden mukaan.

Sivu 70 viides kappale; Puhtaat tietoverkot

Arviota Suomen verkkojen puhtaudesta on käytetty mietinnössä osittain harhaanjohtavalla tavalla.

Viestintäviraston kyberturvallisuuskatsauksessa 1/2014 virasto esittää kysymyksen: Onko Suomessa maailman puhtaimmat verkot? Katsauksen tekstin mukaan ”Suomi on pärjännyt hyvin kansainvälisten tietoturvayhtiöiden julkaisemissa haittaohjelmatilastoissa. Hyvän menestyksen taustalla on Suomessa tehty aktiivinen haittaohjelmien torjuntatyö.
[…]
Suomi oli vuoden 2013 toisella neljänneksellä tietoturvan kärkimaa Microsoftin 20.2.2014 julkaiseman SIR-raportin (Security Intelligence Raport) perusteella. Microsoft on vuodesta 2006 lähtien julkaissut puolivuosittain Security Intelligence Report -nimellä kulkevan tietoturvakatsauksen, jossa arvioidaan tietoturvallisuuden tilaa ympäri maailmaa Microsoftin omien havaintojen perusteella. Raportin mukaan Suomesta löytyi vähiten haittaohjelmien tartuttamia tietokoneita. Suomi on pitkään

sijoittunut Microsoftin raportissa kärkimaiden joukkoon. Edellisen kerran Suomi sijoittui ensimmäiseksi vuoden 2011 ensimmäisellä puoliskolla ja vuonna 2010 (kuva).



Kuva 1 Suomen sijoitus Microsoftin SIR-raporteissa vuosineljänneksittäin (sija 1 on paras)

Myös useat muut tietoturvayritykset kokoavat ja julkaisevat tilastoja eri maista havaituista haittaohjelmista ja tietoturvaloukkauksista. Suomi on sijoittunut kärkimaiden joukkoon myös näissä tilastoissa. Esimerkiksi vuotta 2013 koskevissa Kaspersky Lab- ja Panda Lab -tietoturvayritysten julkaisemissa raporteissa Suomi sijoittui sijalle 3. F-Securen haittaohjelmahavaintotilastossa Suomi sijoittui vuonna 2013 sijalle 2, eli Suomessa havaittiin toiseksi vähiten haittaohjelmia kaikista maista."

Jokainen raportti liittyy pääsääntöisesti sen julkaisseen tahon oman sensoriverkoston tuottamiin tietoihin. Havaintotietoja voidaan näiltä osin pitää eri maiden osalta keskenään vertailukelpoisina, joten maakohtaiset erot eivät selity havaintokykyyn liittyvillä tekijöillä. Eroja saattaa syntyä esimerkiksi kyseisen toimijan markkinaosuudesta tarkasteltavassa maassa.

Viittauksella puhtaisiin tietoverkkoihin ei siis ole varsinaisesti mitään tekemistä sen kanssa, kohdistuuko Suomeen hyökkäyksiä tai ovatko suomalaiset vakoilun tai muun vastaavan kyberympäristössä tapahtuvan toiminnan kohteena.

Mietinnön viittaus puutteelliseen havaintokykyyn voi olla oikea, mutta mietinnössä esitetyt perustelut eivät tätä osoita. Perustelut ovat näiltä osin vailla merkitystä.

FRA-lain vaikutukset

Katso jäljempänä erillinen kohta 5, jossa tarkastellaan mietintöön sisältyvää FRA-lain vaikutusarviointia.

Taloudelliset vaikutukset

Tietoliikennetiedustelun käyttöönottoon ja käyttöön liittyvät kustannukset saattavat olla kansantaloudellisesti merkittäviä. Kustannusten euromäärää ei mietinnössä ole arvioitu lainkaan. Voidaan kuitenkin olettaa, että järjestelmän tiedustelukyvykkyyden perustamiseen liittyvät investointikustannukset ovat vähintään suuruusluokkaa 100 miljoonaa.

Kustannusten suuruudella voi olla ratkaiseva vaikutus järjestelmän hyötyjä ja haittoja punnittaessa.

5 FRA-lain vaikutusarvioinnista

Mietinnön liitteenä oleva vaikutusarviointi ei luo todellista pohjaa asian tarkastelulle mm. seuraavista syistä:

"*Kuvio [1]* ei erikseen kerro IT-sektorin investointien määrään muutoksista, mutta niiden katsotaan seuraavan samanlaista kehitystä pohjautuen alan asiantuntijoiden kommentteihin." (kohta 3.1 sivu 87)

Kuviolla kuitenkin perustellaan sitä, että FRA-lailla ei olisi ollut vaikutusta investointeihin. Tulkinta kuitenkin perustuu itse lauseessa esitettyyn oletukseen, jota ei ole pystytty perustelemaan/perusteltu muuten kuin viittaamalla joihinkin asiantuntijoihin. Arvion merkitys voitaneen perustellusti kyseenalaistaa.

Kuvion 2 avulla perustellaan samaa lopputulosta, mutta toisesta näkökulmasta. Perustelu on kuitenkin vähintään yhtä kyseenalainen kuin kuvion 1 perusteella esitetty.

Mietinnön liitteessä on pyritty myös arvioimaan *FRA-lain vaikutuksia T&K-toimintaan*. Kytkentä T&K-toiminnan ja FRA-lain vaikutusten välillä on vähintäänkin keinotekoinen: miksi FRA-lailla olisi ylipäätään ollut mitään vaikutusta tutkimus- ja kehitystoimintaan? Korrelaation puutteesta johtuen tällä vaikutusarviolla ei ole merkitystä FRA-lain seurausten arvioinnissa.

Tutkimuspanostusten lähderahoitus ei ole tietoliikennetiedustelun näkökulmasta mitenkään relevantti: raha ja siihen liittyvät panostusodotukset eivät ole sidoksissa tietoliikennetiedusteluun muuten kuin erittäin etäisesti - jos edes siten!

Ruotsin kansainvälinen kilpailukykyyn vaikuttavat monet eri tekijät,
joten kehityksen yhdistäminen FRA-lakiin niiden perusteella on mahdotonta.

Taulukossa 3 esitetty riskivertailu datakeskusten sijoituspaikkana sisältää 10 eri tekijää, joiden yhteisarvona määräytyy lopullinen sijoitus. Ruotsin sijoitus vaihtelee ykkössijasta sijaan 26.

Arvioissa on esitetty, että ruotsalaisen lainsäädännön ja pelisääntöjen selkeys saattaa olla jopa kilpailuetu Ruotsille. (Oletettavasti näkemystä perustellaan sillä, että Ruotsi on sijalla kolme arvioitaessa tekijää nimeltä "Political stability". Muihin arvioitaviin tekijöihin esitetty näkemys ei ole liitettävissä.) Perustelu on huono, sillä

poliittisen järjestelmän vakautta arvioitaessa Ruotsin edellä ovat sekä Norja (1) että Suomi (2). Näiden maiden tiedusteluun liittyvät normit ovat täysin erilaiset niin keskenään kuin Ruotsiinkin verrattuna. FRA-lainsäädäntöön liittyvät johtopäätökset ovat vähintäänkin hatarat.

Ruotsia (3) ja Suomea (9) on verrattu vaikutusarviossa toisiinsa ja Ruotsin paremman sijoituksen on esitetty osaltaan johtuvan mahdollisesti pelisääntöjen selkeydestä. Taulukon lähempi tarkastelu kuitenkin osoittaa, että Suomen heikompi sijoitus johtuu ensisijaisesti energiaturvallisuudesta (Energy security; Suomi 30, Ruotsi 15), kansainvälisistä tietoliikenneyhteyksistä (International bandwith; Suomi 22, Ruotsi 10) sekä koulutuksesta (Education; Suomi 15, Ruotsi 9). FRA-lain vaikutukset eivät heijastu näistä mihinkään.

Uuden yritystoiminnan syntyyn Ruotsissa ja Suomessa liittyvät vaikutusarviot ovat luonteeltaan edellä esitetyn kaltaisia, joten samantapaiset vasta-argumentit liittyvät myös tässä kohdassa esitettyihin näkemyksiin.

Facebook ei välttämättä ole vertailun kannalta paras mahdollinen kohde, sillä kyseinen palvelu on nimenomaisesti tarkoitettu tietojen jakamiseen ja julkaisemiseen. Tiedustelulainsäädännöllä ei tätä taustaa vasten ole mitään relevanssia vaikutusarvion tarkoittamassa tarkastelussa.

FRA-lain vaikutuksia erilaisille yrityksille tai yritysryhmille Ruotsissa on kuvattu mietinnön liitteessä seuraavasti: ”Lain todelliset vaikutukset liiketoimintaan ovat kuitenkin olleet vähäiset tai jääneet kokonaan toteutumatta."

Kyseessä on yksittäinen väite, jolle ei ole esitetty minkäänlaisia perusteluja. Yhtä vahvasti voitaneen väittää myös toisin päin: vaikutukset ovat olleet dramaattiset. Tälle näkemykselle on yhtä hatarat perustelut.

Suuri osa vaikutusarvioissa viitatuista *Ruotsin IT-investoinneista* liittyy ruotsalaisten yritysten kotimaisiin investointeihin. FRA-lailla ei voine katsoa olevan mitään merkitystä kyseisen investointitoiminnan kannalta.

FRA-lain vaikutusten arvioinnissa pitäisi olla kyse ensisijaisesti ulkomaisten yritysten Ruotsiin rakentamista kansainvälisistä datakeskuksista, joissa käsitellään muiden kuin ruotsalaisten tietoja. Bahnhof lienee "oikeanlainen" referenssi. FRA-aikajanan mukaan kyseinen yritys on kuitenkin ilmoittanut, että se ei noudata FRA-lakia. Tästäkään yritysesimerkistä ei siis voida tehdä sellaista johtopäätöstä, että kyseisestä lainsäädännöstä olisi syntynyt Ruotsille kilpailuetua.