Puolustusministeriö
Kirjaamo

Viite: Lausuntopyyntö FI.PLM.2015-218, 909/40.02.00/2013

Microsoft Oy:n lausunto tiedonhankintalakityöryhmän mietintöön

Puolustusministeriö on pyytänyt lausuntoja tiedonhankintalakityöryhmän mietinnöstä ”Suomalaisen tiedustelulainsäädännön suuntaviivoja” 9.2.2015 päivätyllä lausuntopyynnöllä. Lausuntopyynnössä pyydetään erityisesti kommentoimaan kehittämisehdotuksia ja johtopäätöksiä (luvut 6 ja 7) ja ehdotusten vaikutuksia lausunnonantajan toimintaan ja toimialalla.

Microsoft Oy kiittää mahdollisuudesta lausua tiedonhankintalakityöryhmän mietinnöstä ja toteaa seuraavaa.

1 Mietinnössä esitetyt kehittämisehdotukset

Mietinnössä esitetään kolme tiedonhankinnan kehittämisaluetta: tietoliikennetiedustelu, ulkomaan henkilötiedustelu ja ulkomaan tietojärjestelmätiedustelu.

Tietoliikennetiedustelulla mietinnössä tarkoitetaan Suomen rajat ylittävien tietoliikenneyhteyksien kautta tapahtuvan viestinnän automaattista koneellista seurantaa ja suodattamista ja tiedusteluviranomaisen tekemää suodatetun tiedon käsittelyä ja analysointia kansallista turvallisuutta uhkaavia toimijoita ja toimintaa koskevan tiedon hankkimiseksi. Tarkoituksena olisi ylimmän valtiojohdon päätöksenteon tukeminen välttämättömällä tilannekuvatiedolla.

Tietoliikennetiedustelu-termin käyttäminen tällaisesta toiminnasta on omiaan johtamaan lukijaa harhaan. Sen vuoksi esitämme termin korvaamista paremmin asiaa kuvaavalla **Viestintätiedustelu**-termillä, jota myös käytämme tässä lausunnossa.

Ulkomaan henkilötiedustelulla mietinnössä tarkoitetaan henkilökohtaiseen kanssakäymiseen tai henkilön tai muun kohteen henkilökohtaiseen havainnointiin perustuvaa tiedonhankintaa.

Ulkomaan tietojärjestelmätiedustelulla mietinnössä tarkoitetaan ulkomaisissa tietojärjestelmissä käsiteltävän tiedon hankintaa tietoteknisin menetelmin eli aktiivista tunkeutumista tietojärjestelmiin ja tietojen keräämistä järjestelmistä. Mietinnössä on rajattu aktiiviset hyökkäystoimet kuten tietojärjestelmien vahingoittaminen, tietojen tuhoaminen tai muuttaminen määritelmän ulkopuolelle.

2 Yleistä

Teknologian kehitys ja uudet innovaatiot mahdollistavat yhä paremmin ajasta ja paikasta riippumattoman viestinnän. Kehitys parantaa ratkaisevasti tuottavuutta, luo uusia työpaikkoja ja edesauttaa talouden kasvua. Kasvu toteutuu kuitenkin vain, jos huolehdimme siitä, että viestintäyhteydet paranevat, datan esteetön liikkuvuus rajojen yli mahdollistetaan ja pilviteknologian hyödyt otetaan käyttöön. Tämä on kuitenkin mahdollista vain käyttäjien luottaessa siihen, että tietoyhteiskunnan palvelut ovat toimintavarmoja ja ne suojaavat käyttäjien perusoikeuksia kuten oikeutta yksityiseen viestintään riittävällä tavalla.

Digitaalinen talous ulottuu viestintä- ja tuottavuuspalveluiden ulkopuolelle kaikkialle teollisuuteen ja palveluihin. Digitaalisuuden täysimääräinen hyödyntäminen kaikilla teollisuuden aloilla on avain suomalaisen teollisuuden kilpailukyvyn ja tuottavuuden parantamisessa sekä talouden kasvun edistämisessä.

Digitalisaatio on muuttanut myös Suomeen ja suomalaisiin kohdistuvien uhkien luonnetta. Verkkorikollisuus on globaalia ja monet valtiolliset toimijat operoivat tietoverkoissa valtioiden rajoista välittämättä.

Tällaisessa jatkuvasti muuttuvassa toimintaympäristössä on entistäkin tärkeämpää, että jokainen toimija vastaa osaltaan turvallisuuden toteuttamisesta. Turvallisuutta ei voi ulkoistaa. Yritysten ja viranomaisten on varmistettava hallussaan olevien tietojen ja tietojärjestelmien riittävä suojaus ja käytettävä palveluiden toteuttamiseen luotettavia palveluntarjoajia. Toimijoilla on oltava riittävät valtuudet tehtäviensä hoitamiseen. Yritysten ja viranomaisten on toimittava yhteistyössä yhteisen tilannekuvan muodostamiseksi. Tilannekuvan on oltava kaikkien toimijoiden käytettävissä. Viranomaisten on kerrottava yrityksille viranomaisten tietoon saadut yrityksiin kohdistuvat uhat.

Mietinnössä on käsitelty useita eri asiakokonaisuuksia, jotka liittyvät toisiinsa varsin löyhästi. Esitetyt jatkotoimenpiteet on kuvattu varsin yleisluontoisesti, minkä vuoksi mahdollinen jatkovalmistelu voi johtaa lopputulokseen, jota mietinnössä ei ole kuvattu.

Pidämme hyvänä sitä, että työryhmä on tehnyt työtään varsin avoimesti ja kuullut laajasti eri osapuolia. Mahdollisessa jatkovalmistelussa tulisi valmistelun avoimuutta vielä parantaa ja varmistaa kaikkien osapuolien mahdollisuus osallistua työskentelyyn haluamassaan laajuudessa.

3 Tiedustelulainsäädännön jatkovalmistelusta

Jatkotyössä on syytä arvioida tiedustelulainsäädännön kehittämistarpeita. Mahdollisen lainsäädännön on oltava mahdollisimman selväsanaista ja yksitulkintaista, jotta toimintaympäristö säilyy ennustettavana sekä Suomessa jo toimivien että investointipäätöksiä harkitsevien yritysten kannalta. Mietinnössä esitetyt lainsäädäntöhankkeet tulisi valmistella erikseen kussakin vastuuministeriössä. Microsoft Oy on kiinnostunut osallistumaan tiedustelulainsäädännön jatkovalmisteluun.

Valmistelussa tulee ottaa huomioon tiedustelu- ja viranomaistoiminnan kehittämistä tietoverkoissa ohjaavat yleiset periaatteet. Periaatteet on lyhyesti esitetty luvussa 4 ja laajemmin sivustolla http://reformgovernmentsurveillance.com.

3.1 Viestintätiedustelu

Viestintätiedustelun mahdollinen tarve tulee selvittää yleisellä tasolla osana tiedustelulainsäädännön valmistelutyötä. Viestintätiedustelua koskevan erityislain valmistelu voitaneen aloittaa tiedustelulainsäädännön käsittelyn jälkeen, mikäli toiminnan tarpeellisuudesta, hyödyistä ja kustannuksista sekä vaikuttavuudesta saavutetaan riittävän laaja yhteinen objektiivinen faktoihin perustuva näkemys. Erityisesti tästä syystä yritysten osallistuminen jatkotyöskentelyyn on tärkeää.

Mikäli viestintätiedustelua koskevaa lainsäädäntöä aletaan jossain tulevaisuuden hetkessä valmistella, valmistelussa tulee pitää ohjaavina periaatteina mietinnössä ansiokkaasti esitetyt yritysten ja organisaatioiden toimintaa koskevat seikat täydennettyinä seuraavasti:

- Ohjelmistovalmistajia ja palveluntuottajia ei tule velvoittaa toteuttamaan ohjelmistoihin tai palveluihin takaportteja
- Organisaatioita ei tule velvoittaa luovuttamaan salausavaimia viranomaisille tai auttamaan viranomaisia salausten purkamisessa. Lainsäädäntöön ei saa sisällyttää salausmenetelmien tai

muiden viestinnän luottamuksellisuutta turvaavien ja viestinnän osapuolia suojaavien menetelmien käyttökieltoja tai käyttörajoituksia.

- Viestintätiedustelun kohteena saa olla vain teleyritysten julkisten verkkojen Suomen rajat ylittävä liikenne. Viestintätiedustelua ei tule ulottaa organisaatioiden yksinomaisessa käytössä oleviin tietoliikenneyhteyksiin.
  Mikäli valmistelussa pidetään esillä mahdollisuutta, että viestintätiedustelu voitaisiin ulottaa organisaatioiden yksinomaisessa käytössä oleviin tietoliikenneyhteyksiin, tällä olisi varmasti Suomen kannalta kielteinen vaikutus datakeskusinvestointeja ja ICT-palvelujen sijoituspaikkoja harkitsevien toimijoiden päätöksiin. Tämä vaikutus voisi kestää hyvinkin pitkään, sillä viestintätiedustelua koskevan lainsäädännön valmistelu- ja käsittelyaika on todennäköisesti pitkä asiaan liittyvien perustuslaillisten näkökohtien vuoksi.
- Tiedusteluviranomaisten tulee vastata täysimääräisesti mahdollisen viestintätiedustelun kustannuksista. Kustannuksia ei osittainkaan saa sälyttää yritysten kannettaviksi

Tiedustelulainsäädännön valmistelutyössä on tarkoin pidettävä mielessä, että toiminnan tarkoituksena on valtiojohdon päätöksentekokyvyn mahdollistaminen. Tämän vuoksi olisikin harkittava sitä, että myös toiminta olisi tiukasti valtiojohdon ohjauksessa. Tiedustelutoiminta rikkoo hyvinkin helposti muiden maiden lainsäädäntöä. Toimenpiteiden käynnistäminen vaatii poliittista harkintaa. Ratkaisut voitaisiin tehdä esimerkiksi ulko- ja turvallisuuspoliittisessa valiokunnassa tapauskohtaisesti.

3.2 Ulkomaan tietojärjestelmätiedustelu

Mahdolliseen ulkomaan tietojärjestelmätiedusteluun liittyy merkittävä periaatteellinen asia. Suomen ratifioimissa kansainvälisissä sopimuksissa tietojärjestelmiin tunkeutuminen on kriminalisoitu ja teot on määritelty kansallisessa lainsäädännössä rangaistaviksi.

Voidaan aiheellisesti kysyä, kasvaisiko kansalaisten ja yritysten luottamusta verkkoon ja sen palveluihin, jos viranomaisille sallittaisiin tällainen toiminta.

Suomi on toimillaan kansainvälisessä yhteisössä rakentanut menestyksekkäästi mainetta yhteistyön rakentajana ja rauhansovittelijana. Tätä taustaa vasten olisikin luontevampaa, että Suomi ottaisi kansainvälisillä foorumeilla aktiivisen roolin tietojärjestelmien turvallisuuden edistämisessä ja edistäisi laajasti hyväksyttyjen oikeushyvien turvaamista digitaalisessa toimintaympäristössä.

Suomi voisi toimia aktiivisesti erityisesti kansainväliseen oikeusapumekanismiin liittyvien toimintatapojen uudistamisessa ja mekanismin siirtämisessä globaalisti digiaikaan sekä valtioiden lainsäädäntöjen eroavuuksista johtuvien ristiriitojen ratkaisemiseen kykenevien foorumien luomisessa.

Microsoft tarjoaa palveluita globaalisti yrityksille, valtioiden viranomaisille ja kuluttajille ja suojaa asiakkaidensa tiedot mahdollisimman hyvin sekä pyrkii kaikin käytettävissä olevin laillisin keinoin estämään palveluihin tunkeutumisen ja asiakkaiden tietojen hyväksikäytön. Suhtaudumme valtiollisten toimijoiden tunkeutumisyrityksiin samalla tavalla kuin muuhunkin verkkorikollisuuteen: estämme ja torjumme tunkeutumisyritykset päättäväisesti.

3.3 Mietinnön asiasisältö

Mietintö vaikuttaa lainsäädäntöä koskevien osuuksien osalta hyvin ja perusteellisesti valmistelulta. Näitä osuuksia voidaan käyttää hyvin jatkovalmistelun lähdemateriaalina.

Teknologian, tietoverkkojen, tietojärjestelmien, haittaohjelmien ja niiden havainnoinnin osalta mietinnön teksti on naivistista, perustuu vanhentuneisiin käsityksiin ja yksinkertaistettuihin mielikuviin. Teksti sisältää runsaasti virheellisyyksiä, perustelemattomia väitteitä ja mielipiteitä. Mietintöä ei näiltä osin tule käyttää

valmistelun lähdemateriaalina, vaan valmistelun tulee perustua faktoihin ja objektiiviseen analyysiin tilanteesta ja tarvittavista toimenpiteistä.

Luvussa 5 on näytteenomaisesti esitetty ja kommentoitu muutamia mietinnön tekstin pahimpia kömmähdyksiä.

4 Tiedustelutoimintaa ja viranomaisten tiedonhankintaa ohjaavat periaatteet

Microsoft on yhdessä muiden suurten tietotekniikkatoimittajien kanssa koostanut luettelon periaatteista, joita tulisi noudattaa kehitettäessä tiedustelutoimintaa ja viranomaisten tiedonhankintaa Internetistä ja pilvipalveluista koskevaa lainsäädäntöä. Periaatteet on tuotu esiin Yhdysvaltain liittovaltion tiedustelutoimintaa koskevan keskustelun yhteydessä. Ne on tarkoitettu kaikille valtioille, myös Suomelle. Periaatteiden tarkoituksena on turvata Internetin kehittyminen globaalina, kaikkien yksilöiden ja organisaatioiden käytettävissä olevana palveluna.

Esitämme, että Suomen valtion tulisi ottaa nämä periaatteet ohjenuoraksi tiedustelulainsäädännön kehitystyössä.

4.1 Viranomaisten oikeutta kerätä käyttäjien tietoja tulee rajoittaa

Valtioiden tulisi säätää järkevät rajoitukset viranomaisten toimivallalle kerätä käyttäjien tietoja palveluntuottajilta. Tietojen keruu tulee tapahtua vain tarkoin rajatuissa olosuhteissa ja se tulee tasapainottaa käyttäjien kohtuullisten yksityisyydensuojan odotusten kanssa ottaen huomioon toiminnan vaikutukset yksilöiden Internetiä ja verkkopalveluita kohtaan tuntemaan luottamukseen. Viranomaisten valvonnan tulee kohdistua vain lainsäädännössä määritellyillä perusteilla yksilöityjen käyttäjien tietoihin eikä viranomaisten tule kerätä tietoja tietoverkoista rajoituksetta.

4.2 Tiedonkeruun tulee olla valvottua ja vastuullista

Viranomaisten tietopyyntöjä ja tiedonkeruuta varten tulee olla selkeä lainsäädäntökehikko, jonka perusteella viranomaisten valtuuksia ja toimenpiteitä valvotaan riittävällä tarkkuudella. Toimintaa valvovien toimielimien tulee olla riippumattomia ja valvonnan kohteilla ja tietopyyntöjen vastaanottajilla tulee olla mahdollisuus valittaa päätöksistä. Viranomaisten ja valvontaelinten keskeiset päätökset tulee julkistaa viivytyksettä, jotta kansalaisvalvonta olisi mahdollista.

4.3 Tietopyyntöjä koskevan toiminnan tulee olla läpinäkyvää

Viranomaisten toimivaltuuksia ja valtuuksien perusteella toteutettavia valvontaohjelmia koskevan keskustelun mahdollistamiseksi toiminnan on oltava läpinäkyvää. Viranomaisten tulee antaa yritysten julkistaa erilaisten tietopyyntöjen lukumäärät ja luonne. Lisäksi viranomaisten itsensä tulee julkistaa vastaavat tiedot.

4.4 Vapaata tiedonkulkua tulee kunnioittaa

Valtioiden rajat ylittävä tietoliikenne on olennainen edellytys tämän vuosisadan globaalin talouden toiminnalle. Viranomaisten tulee sallia tiedon kulku tietoverkoissa. Lisäksi viranomaisten ei tule rajoittaa yksittäisten käyttäjien ja yritysten pääsyä laillisesti saatavissa olevaan toisten valtioiden alueella sijaitsevaan tietoon.

4.5 Valtioiden väliset mahdolliset ristiriidat tulee ratkaista

Jotta lainsäädännön ristiriitaisuuksilta vältyttäisiin, valtioiden tulee rakentaa kestäviä periaatteita noudattava ja läpinäkyvyyttä edistävä kehikko rajat ylittävien tietopyyntöjen hallintaan esimerkiksi vahvistamalla olemassa olevia maiden välisiä virka-apusopimuksia. Valtioiden tulee sopia keskenään

menettelytavoista, joilla ratkaistaan eri maiden lainsäädäntöjen mahdollisista ristiriitaisuuksista aiheutuvat ongelmat.

5 Havaintoja mietinnön sisällöstä

5.1 Kohta 5.1 sivu 46 Sähköinen viestintäteknologia ja kansalliseen turvallisuuteen kohdistuvat uhat

”Tietoverkkouhkien ja uhkia koskevan viestinnän havaitseminen, niiden taustalla olevien tahojen tunnistaminen ja uhan luonteen selvittäminen muodostaa edellytyksen sille, että kansallista turvallisuutta vaarantavien tekojen toteutuminen voidaan estää.”

Väite ei pidä paikkaansa. Tietoverkkouhkia, myös kansallista turvallisuutta uhkaavia, voidaan estää ja estetään menestyksekkäästi vaikka uhkien taustalla olevista tahoista ei ole tietoa. Analogiana: lukko ovessa suojaa kaikilta sisäänpyrkijöiltä. Toki uhkien taustalla olevien toimijoiden selvittäminen auttaa pitkällä aikavälillä uhkien poistamisessa normaalin kansainvälisen poliittisen toiminnan kautta.

5.2 Kohta 5.2 sivut 46 - 47 Organisaatioiden mahdollisuuksia havainnoida niihin kohdistuvia tietoverkkouhkia

Luvun teksti on tarkoitushakuista ja sisältää runsaasti asiavirheitä:

”… säädetään tietoyhteiskuntakaaren 272§:ssä. Säädös antaa yrityksille, yhteisöille ja viranomaisille työkaluja niihin kohdistuvien kybertekojen havaitsemiseksi ja torjumiseksi.” Teksti jättää avoimeksi sen, ovatko laissa esitetyt keinot riittäviä ja antaa ymmärtää että keinot eivät ole riittäviä. Tämän vihjauksen tueksi ei kuitenkaan esitetä aineistoa.

Tekstistä on jätetty pois olennaisia seikkoja: lainkohta kuuluu (272§ 1 mom 1 kohta) ”*… häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi.*” Tietoturvatoimenpiteiden suorittajan näkökulmasta syyt, olosuhteet, tekijät ja taustat ovat yhtä keskeisiä asioita kuin muutkin tietoturvatapahtuman tiedot. Näiden selvittäminen kuitenkin kuuluu esitutkintaviranomaiselle eikä tapahtuman kohteena olleelle organisaatiolle. Esitutkintaviranomaisella on laissa turvattu tarvittavat valtuudet tutkinnan suorittamiseen ja kohteena olevalla organisaatiolla on tietoyhteiskuntakaaren nojalla oikeus kerätä esitutkinnassa tarvittavat tiedot. Kohdan 5.2 viimeinen kappale ei siis pidä paikkaansa.

”Havainnointitoimenpiteet suoritetaan hajautetusti, jolloin niiden laatu ja taso vaihtelevat *organisaatiokohtaisesti.”* Lause on helppo ymmärtää todeksi. Tässä yhteydessä siitä kuitenkin saa sellaisen kuvan, että laatu ja taso eivät ole riittäviä eikä niitä pystytä korjaamaan. Tosiasiassa kunkin toimijan tulee mitoittaa vastatoimenpiteensä kokemien uhkien ja riskien mukaisesti. Keskitetyssä toimintamallissa havainnointitoimenpiteet ovat osalle toimijoista ylimitoitettuja ja kriittisimmille alimitoitettuja. Erityisesti kriittisimpien toimijoiden osalta keskitetty ratkaisu johtaa usein valheelliseen turvallisuuden tunteeseen.

”*Haittaohjelmista vaikeimmin havaittavia ja samanaikaisesti suurinta vahinkoa kansalliselle turvallisuudelle aiheuttavia ovat valtiolliset vakoilu- ja muut haittaohjelmat. Tällaisia haittaohjelmia koskevat tunnisteet ovat sellaista korkean suojaustason tietoa, jota vaihdetaan tyypillisesti osana turvallisuus- ja tiedustelupalveluiden kansainvälistä yhteistyötä.*”

Kappaleessa on useita virheellisyyksiä. Vaikeimmin havaittavia ovat tuntemattomat haittaohjelmat riippumatta siitä, kuka haittaohjelman takana on. Jos haittaohjelmasta on olemassa tunnisteita, se ei enää ole vaikeasti havaittava.

Vaikeasti havaittavia haittaohjelmia tunnistetaan ja torjutaan ohjelmien käyttäytymiseen perustuvalla analyysilla, jossa voidaan jopa pakottaa haittaohjelma kaatumaan. Käyttäytymiseen perustuvaa

haittaohjelmien torjuntaa voidaan toteuttaa parhaiten kohteena olevan organisaation sisäverkossa ja työasemissa.

Väitettä siitä, että turvallisuus- ja tiedustelupalveluilla olisi käytettävissä kaupallisille toimijoille tuntemattomien haittaohjelmien tunnisteita, on käytännössä mahdoton todistaa oikeaksi tai vääräksi. Kaupalliset haittaohjelmien torjuntaohjelmistot tunnistavat myös kaikki tunnetut valtiollisten toimijoiden liikkeelle laskemat haittaohjelmat.

On mahdollista, että turvallisuus- ja tiedusteluorganisaatiot pystyisivät tunnistamaan ja eristämään haittaohjelmia ilman tietoturva-alan yritysten apua. Kaikissa tunnetuissa tapauksissa yritykset ovat kuitenkin olleet tiiviisti mukana löytämässä ja analysoimassa valtiollisten toimijoiden tuottamia haittaohjelmia.

5.3 Kohta 5.3 sivu 47 Tiedonhankintavaltuudet

"… ettei salaisia tiedonhankintakeinoja voida nykyisin käyttää pelkän tiedustelutiedon hankkimiseen sellaisesta esimerkiksi kansallista turvallisuutta uhkaavasta toiminnasta, joka ei ole edennyt rikoksen valmistelun asteelle tai ei ole säädetty rangaistavaksi."

Raportissa aivan oikein todetaan, että turvallisuusviranomaiset eivät voi käyttää salaisia tiedonhankintakeinoja kansalaisten laillisen toiminnan seuraamiseen. Tekstin muotoilusta voi satunnainen lukija saada käsityksen, että viranomaisten tulisi voida käyttää salaisia pakkokeinoja kansalaisten laillisen toiminnan seuraamiseen, jos viranomaiset kokevat toiminnan uhkaavaksi. Tällaisten avoimeen laillisuuteen perustuvaan yhteiskuntaan täysin soveltumattomien näkemysten leviäminen on omiaan heikentämään kansalaisten luottamusta turvallisuusviranomaisten toimintaan.

5.4 Kohta 6.1.7 sivu 69 Tietoliikennetiedustelun vaikutusarviointia

"Tietoliikennetiedustelu myös 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."

Väite ei pidä paikkaansa. Tietoverkossa tapahtuvalla valvonnalla on pienemmät mahdollisuudet havaita vakoilu- ja haittaohjelmia kuin hyvin toteutetulla kohteena olevan organisaation sisäverkossa tapahtuvalla haittaohjelmien käyttäytymiseen perustuvalla valvonnalla ja analyysilla.

Sivu 70: *"Arvion puhtaista tietoverkoista kyseenalaistaa Kyberturvallisuuskeskuksen raportti, jonka mukaan kyberhyökkäyksiä järjestelmällisesti seuraavissa länsimaissa havaitaan vuosittain kymmeniä kybervakoilutapauksia, joissa teknisenä apukeinona on käytetty kohdistettua haittaohjelmaa. Raportin mukaan uhka kohdistuu myös Suomeen. Näistä maista poiketen Suomessa ei tällä hetkellä ole järjestelmää, jolla erityisen vakavia kohdennettuja haittaohjelmahyökkäyksiä voitaisiin seurata. Näin ollen voidaan arvioida, että käsitys erityisen puhtaista tietoverkoista perustuu ainakin vakavimpien kybertekojen osalta puutteelliseen kansalliseen havaitsemiskykyyn. Suomen tietoliikennetiedustelukyvyn kehittämisen voidaan arvioida nostavan kynnystä kohdistaa maahamme kybervakoilua."*

Käsitys Suomen tietoverkkojen puhtaudesta ja haittaohjelmien vähäisestä määrästä perustuu muiden tietojen lisäksi ainakin Microsoftin puolivuosittain julkaisemaan raporttiin, jossa analysoidaan havaintojen perusteella haittaohjelmien levinneisyyttä ja uhkien kehittymistä. Raportti perustuu yli 600 miljoonan tietokoneen (käyttäjän luvalla) lähettämiin tietoihin.

Suomi on säännönmukaisesti ollut raportissa haittaohjelmahavaintojen ja haittaohjelmatartuntojen suhteellisen osuuden vähäisyydessä maailman parhaiden maiden joukossa, usein ensimmäisenä tai toisena. Suomen tiedot ovat vertailukelpoisia muiden maiden tietojen kanssa.

Nykyiset järjestelmät havaitsevat valtiollisia vakoilu- ja haittaohjelmia samalla tavalla kuin muitakin edistyneitä haittaohjelmia (APT, advanced persistent threat). Näiden löytäminen on yleensä työtä, jossa tarvitaan huomattava määrä tapahtumatietoa organisaation työasemista ja osaavia analyytikkoja ja tietoturvatutkijoita. Kun joku toimija löytää tällaisen haittaohjelman, kansainvälisellä yhteistyöllä varmistetaan, että kaikki markkinoilla olevat suojausohjelmistot havaitsevat ja estävät haittaohjelman toiminnan.