Puolustusministeriö

**Lausunto tiedonhankintalakityöryhmän mietintöön tiedustelulainsäädännöstä**

FICIX ry kiittää mahdollisuudesta saada lausua tiedonhankintalakityöryhmän mietintöön tiedustelulainsäädännöstä.

**Yleistä**

Tiedustelutiedon hankkimisen ja käyttämisen pelisäännöt ovat nousseet kansainväliseen keskusteluun kesän 2013 jälkeen ja edelleen kiihtyvät uusien tiedustelutapausten julkitulon myötä. FICIX ry pitää kannatettavana, että oikeusvaltion periaatteita noudatetaan selvittämällä jo voimassaolevan lain ja sääntelyn antamat mahdollisuudet sekä mahdollisuus edetä niitä kehittämällä. FICIX ry pitää itse mietintöä ammattimaisesti toteutettuna ja varsin kattavana. Puutteeksi voidaan katsoa elinkeinoelämän ja kansalaisyhteiskunnan edustajien poissulkeminen ryhmästä vastoin näiden tahojen nimenomaista pyyntöä osallistua.

FICIX ry tunnustaa, että moderni ja demokraattinen tietoyhteiskunta on uusien ja lisääntyvien uhkien edessä toimintojen siirtyessä tietoverkkoihin yhä enenevissä määrin. Turvallisuutta ja varautumista tulee jatkuvasti kohentaa ja viranomaisten toimintavaltuuksia sekä -edellytyksiä ylläpitää riittävässä määrin. Turvallisuus ei kuitenkaan ole missään tilanteessa absoluuttista joten äärimmäisiä keinoja ja menetelmiä ei tule ottaa käyttöön vaan pyrkiä tasapainoiseen tilanteeseen jossa kansalaisten ja yhteiskunnan turvan tason voidaan katsoa olevan tasapainossa niiden arvojen kanssa jotka suomalainen yhteiskunta hyväksyy.

Tietoverkkojen ja –tekniikan, kyber-ympäristön, uhkia ja mahdollisuuksia pohdittaessa olisi hyvä tiedostaa, että toimialan kaikki sovellukset ja infrastruktuuri ovat kaksoiskäyttöön soveltuvia kaikilta osiltaan. Järjestelmä tai toiminto joka on suunniteltu tiettyä tarkoitusta varten voidaan valjastaa päinvastaiseen käyttöön tai käyttää toisen järjestelmän osana niin hyvässä kuin pahassa. Tiedonhankintaan liittyvät järjestelmät eivät ole tähän poikkeus vaan yksi tekijä lisää. Esimerkkinä tiedonhankintajärjestelmän väärinkäytöstä on disinformaation syöttö turvallisuusviranomaisten päätösketjuun.

**FICIX ry:n keskeiset huomiot ja viestit**

Johtopäätösten osassa 7.1. ehdotetaan toimivaltuuksien kehittämistä rajat ylittävään liikenteeseen. Käytännössä tämä tarkoittaa tiedustelun toteuttamista valtion itärajalla sekä länsirajalla Maarianhaminassa, jotka ovat keskeisiä paikkoja rajat ylittäviin yhteyksiin. Tiedustelun toteuttaminen Suomen manneralueella jättäisi Ahvenanmaalaiset oman valtion tiedustelun piiriin jota voidaan pitää syrjivänä toimintana. Tiedustelun toteuttajan osalta on tarpeen selvittää myös ko. organisaation toimintavaltuudet demilitarisoidulla ja vahvan itsehallinnon omaavalla alueella.

Käytännössä rajat ylittävää liikennettä esiintyy yleisesti myös tavanomaisessa viestinnässä Suomen kansalaisten kesken ja sitä on käytännössä myös mahdoton välttää. Useat suomalaisilta näyttävät Internetin palvelut tuotetaan tosiasiallisesti ulkomailta. Esimerkiksi *www.google.fi* hakukone vastaa Tukholman alueelta suomalaisten käyttäjien hakuihin. Palvelussa käytetyt hakusanat, kuten myös käyttäjän saamat vastaukset ja niistä tehdyt valinnat, ovat Suomen ulkopuolella seurattavissa.

Suomen oma Internetin maatunnus .fi on globaalisti hajautettu Ruotsalaisen Netnod AB:n toimesta. Hajautus palvelee käytettävyyttä ja hyökkäyskestävyyttä mutta samalla mahdollistaa sen, että nimipalvelinkyselyt suomen maajuureen ovat yleisesti seurattavissa useammassakin eri valtiossa Suomen ulkopuolella.

Liikenteen salauksen osalta FICIX ry yhtyy Liikenne- ja Viestintäministeriön mielipiteeseen. Mietinnössä ei ole annettu selvitystä onko Suomella mahdollisuus saada käyttöönsä keskeisiä salausavaimia tiedustelun hyödyllisyyden takaamiseksi.

Suomen kauttakulkuliikenne on toteutettu pääosin valopoluin (DWDM) tai vuokrakaapelein (IRU). Näiden osalta kapasiteetti on pois kansallisesta välityskapasiteetista ja siten niissä kulkevan liikenteen määrä tai laatu ei uhkaa Suomen turvallisuutta millään tavoin. Kauttakulkuliikenteen tiedustelu on siten verrattavissa kokonaan ulkomailla toteutettavaan tiedusteluun.

**Ehdotus tiedustelun toteuttamiseksi vastuullisesti**

Teleyrityksillä, joiden kautta tietoliikenne suomeen ja suomesta hoituu, on lakisääteinen oikeus ja velvollisuus tallettaa viestinnän tietoja sekä laskutusta, palvelukehitystä että viranomaisia varten. Velvollisuutta voidaan laajentaa liikenteen luovutusvelvoitteella, rajattuna valitun lupamenettelyn asettamin kriteerein. Lupamenettelynä voi toimia tuomioistuinlaitos kuten toimii myös telepakkokeinojen oikeuttajana ja lupamenettely voi olla etu- tai jälkikäteistä. Väärin perustein tai oikeudettomaan kohteeseen tehty tiedustelu tai liikenteen luovutus tulee sanktioida. Luonnollisesti liikenteen luovutusvelvollisuutta ei ole teleyrityksellä joka ei hallinnoi rajat ylittäviä telekaapeleita.

Teleyrityksillä on olemassa rekisterit ja keinot estää sellaisten tahojen seuranta joiden katsotaan nauttivan erityistä suojaa demokratiahyveiden takaamisen vuoksi. Rikosepäilyissä nämäkin tahot tietysti ovat rikoslain alaisia ja teletietoihin pääsyn takaa säädetyt telepakkokeinot. Rekistereillä suojattavia tahoja ovat mm. valtion ylin johto, toimittajien lähdesuoja sekä asianajosuoja. Rekistereitä on mahdollisuus myös laajentaa kattamaan kaikkia viestiviä tahoja jotka siihen ilmoittautuvat. Kyberrikolliset joista Suomelle on todellista uhkaa tuskin ilmoittautuvat listalle.

Koska tiedustelulla hankittu tieto on usein salaista tulisi harkita sen tarkastamiseen eettistä toimielintä jolla oikeusturva voidaan taata edes kohtuullisesti oikeusprosesseissa.

Televerkkojen seuranta on mahdollista toteuttaa vastuullisesti, vesittämättä tuloksia ja käsittääksemme myös puuttumatta perustuslailliseen viestinnän suojaan. Vastuullisesti toteutettu valvonta on myös elinkeinoelämän, esim. palvelinkeskusten etu eli valvonnan toteuttamismalli voi toimia myös kilpailuetuna.

**Poliittiset riskit**

Tiedustelulla saadun arkaluontoisen ulkovaltoja koskevan tiedon säilytys ja salassapito kansallisesti sisältää poliittisen riskin. Tietovuoto, joko järjestelmään tunkeutumisella tai henkilövuodolla, voi aiheuttaa ulkopoliittisen kriisin johon Suomen kyky vastata on heikko. Uhkakuvana voi pitää tilannetta, jossa tietovuoto johtaa vaikkapa pakotteisiin kuten kauppasaartoon tai Suomi joutuu sotilaallisen painostuksen alle. Tällaisessa tapauksessa, joista siis on esimerkkejä maailmalta jo, Puolustusvoimien ja Suojelupoliisin toimet tehtäviensä toteuttamiseksi kääntyisivät itseään vastaan – toiminta olisi saattanut Suomen väestön vaaraan tai ollut elinkeinoille haitallinen.

Tiedustelulla saadun tiedon luovutus Suomen ulkopuolelle tulisi altistaa parlamentaariseen ohjaukseen ja valvontaan jotta poliittinen riski voidaan arvioida demokraattisella menettelyllä.

Espoossa, 7.4.2015

FICIX ry

Jorma Mellin

Puheenjohtaja