Eduskunta
Liikenne- ja viestintävaliokunta
LiV@eduskunta.fi

30.5.2018

Viite: Liikenne- ja viestintävaliokunnan lausuntopyyntö HE 61/2018 vp

HE 61/2018 vp Hallituksen esitys eduskunnalle laiksi Liikenne- ja viestintäviraston perustamisesta, Liikennevirastosta annetun lain muuttamisesta ja eräiksi niihin liittyviksi laeiksi

Eduskunnan liikenne- ja viestintävaliokunta on pyytänyt Euroopan hybridiuhkien torjunnan osaamiskeskukselta lausuntoa hallituksen esityksestä eduskunnalle laiksi Liikenne- ja viestintäviraston perustamisesta, Liikennevirastosta annetun lain muuttamisesta ja eräiksi niihin liittyviksi laeiksi. Euroopan hybridiuhkien torjunnan osaamiskeskus lausuu asiassa seuraavaa:

Yleistä hybridiuhkista:

Euroopan turvallisuusympäristö on viime vuosina ollut merkittävien muutosten kohteena. Turvallisuusympäristön muutosta sekä uusia uhkakuvia käsittelevissä keskusteluissa hybridiuhan käsite nousee usein esille.

Hybridiuhkien lisääntyminen onkin osa Euroopan turvallisuusympäristön muutosta. Kyse ei ole vain hybriditaktiikan hyödyntämisestä osana sotilaallista konfliktia, vaan hybridikeinoja käytetään laajemmin osana voimapolitiikkaa. Hybridivaikuttamisella ymmärretään suunnitelmallista toimintaa, jossa valtiollinen tai ei-valtiollinen toimija voi hyödyntää samanaikaisesti erilaisia keinoja vaikuttaakseen kohteena olevan valtion heikkouksiin ja saavuttaakseen omat tavoitteensa. Kyseeseen voivat tulla esimerkiksi sotilaalliset, taloudelliset tai teknologiaan perustuvat painostuskeinot sekä erilaiset informaatio-operaatiot, mukaan lukien sosiaalisen median hyödyntäminen.

Turvallisuusympäristön muutokseen vaikuttavat muutokset useilla eri toimintasektorilla. Muutoksiin maailmanpolitiikan toimintakentässä ovat vaikuttaneet muun muassa suurvaltojen ja kansainvälisten instituutioiden uudet valtasuhteet sekä pyrkimys niiden uudelleen järjestelyyn. Useat valtiot hakevat itselleen joko alueellisen suurvallan tai globaalin suurvallan statusta.

Median toimintakentällä internet, tiedon tuottamisen ja hankkimisen reaaliaikaisuus sekä sosiaalinen media ovat nousseet merkittävään rooliin. Riippuvuus digitaalisesta ympäristöstä sekä siellä tuotetusta informaatiosta on kasvanut. Tämä on johtanut myös uusien ja epäluotettavien lähteiden nopeaan lisääntymiseen sekä luonut tilaa informaatiovaikuttamiselle, sisällönmanipulaatiolle sekä tehokkaalle mielipiteen muokkaukselle. Hybriditoiminnasta puhuttaessa esillä on usein informaatiovaikuttaminen. Se on toimintaa, jolla pyritään järjestelmällisesti vaikuttamaan yleiseen mielipiteeseen, ihmisten käyttäytymiseen ja päätöksentekijöihin sekä edelleen yhteiskunnan toimintakykyyn. Informaatiovaikuttamisen keinoja ovat esimerkiksi väärien tai harhaanjohtavien tietojen levittäminen sekä painostaminen, mutta myös sinänsä paikkaansa pitävän tiedon tarkoitushakuinen käyttö. Kyseessä on strateginen toiminta, jonka tavoitteena

on saada kohde tekemään itselleen haitallisia päätöksiä tai toimimaan omaa etuaan vastaan. Informaatiovaikuttamista on vaikea havaita ja torjua, mikä tekee siitä tehokkaan menetelmän demokraattisia prosesseja vastaan käytettäväksi.

Globalisaatio ja keskinäisriippuvuus ovat edenneet yhä pidemmälle, tehden maailmasta yhä monitasoisemman ja moninaisemmin verkottuneen. Linkki sisäisen ja ulkoisen turvallisuuden välillä vahvistuu edelleen, eikä niitä voi erottaa toisistaan. Uhkat ovat usein luonteeltaan rajat ylittäviä, laajalle levinneitä sekä kompleksisia. Usein ne ovat ennalta arvaamattomia, mikä tarkoittaa, että niihin on vaikea varautua. Keskinäisriippuvuuksien myötä myös haavoittuvuudet lisääntyvät. Valtiollisten ja ei-valtiollisten toimijoiden verkottuminen antaa varjopuolenaan mahdollisuuksia myös hybridivaikuttamiselle, kun erinäisten toimintojen takana olevia tahoja sekä syy-seuraussuhteita on vaikea tunnistaa.

Sodan ja konfliktin kuvat ovat olleet voimakkaan muutoksen kohteena. Siinä missä perinteinen sotilaallinen turvallisuus on edelleen relevantti, on yhtä ilmeistä, että monet asiat ovat muuttuneet. Perinteinen raja sodan ja rauhan sekä kansalaisen ja sotilaan välillä on hämärtynyt. Pienet vihreät tunnuksettomat miehet ovat ylittäneet rajoja, kyberhyökkäyksiä toteutetaan enenevässä määrin, trollijoukkoja valjastetaan informaatiovaikuttamiseen sekä pakolaisvirtoja ohjataan rajojen yli.

Toimintakentillä tapahtuneet muutokset sekä sisäisen ja ulkoisen turvallisuuden entistä tiiviimpi yhteen kietoutuminen ovat mahdollistaneet hybridiuhkilla vaikuttamisen, niiden luomisen ja käytön. Verrattuna aiempaan, myös Suomen turvallisuus kytkeytyy entistä selkeämmin globalisaation muokkaamaan toimintakenttään. Suomen turvallisuutta uhkaavat vakavimmat tekijät liittyvät nykyisin usein Suomen ulkopuolisiin tapahtumiin. Siten myös ulkomaista alkuperää olevan ja siellä syntyvän uhkan seuraukset näkyvät Suomessa aiempaa herkemmin. Kansalliseen turvallisuuteen kohdistuville ulkoisille uhkille on yhteistä se, että taustalla olevien valtiollisten ja ei-valtiollisten tahojen tunnistaminen ja erottaminen toisistaan on yhä vaikeampaa.

Kansalliseen turvallisuuteen kohdistuvina uhkina voidaan pitää muun muassa kansainvälistä terrorismia, ulkovaltojen Suomeen ja sen etuihin kohdistamaa vakoilua, joukkotuhoaseiden ja kaksikäyttötuotteiden levittämispyrkimyksiä sekä sellaista kansainvälistä järjestäytynyttä rikollisuutta, joka pyrkii vaikuttamaan yhteiskunnalliseen päätöksentekoon tai soluttautumaan valtiorakenteisiin. Viime vuosina erityisesti tietoverkkoympäristössä tapahtuva rajat ylittävä vakoilu on noussut merkittäväksi uhkaksi. Tällainen toiminta mahdollistaa suurten tietomäärien hankkimisen keskitetysti, mikä voi aiheuttaa korjaamatonta vahinkoa kohdevaltion turvallisuudelle ja sen eduille. Tietoverkoissa tapahtuva sabotaasi ja tiedon vääristäminen ovat myös merkittäviä uhkia.

Lisäksi valtiolliset toimijat voivat käyttää ohjauksessaan olevia ns. liiketaloudellisia toimijoita Suomea tai muita valtioita vahingoittaviin tarkoituksiin muun muassa liiketoimintaperusteisilla hankinnoilla, joilla ei ole kuitenkaan havaittavaa tuottoa suurille investoinneille. Myös ei-valtiolliset toimijat voivat haluta päästä kohteisiin tai anastaa tietoja. Näin ollen kriittisen infrastruktuurin määritteleminen on erityisen tärkeää. Esimerkiksi merkittävät turvallisuuteen linkittyvät liikenteen-valvontajärjestelmät, olisi turvallisinta pitää omassa hallinnassa. Erilaisissa yhtiöittämisprosesseissa hallinnan menetys on mahdollinen. Lisäksi avainhenkilöstön kansalaisuus- ja lojaliteettiasioiden tarkastelut ja menettelyt ovat olennaisen tärkeitä ennalta estävässä työssä.

Nykyisessä turvallisuusympäristössä uhkien ymmärtäminen sekä oman järjestelmän haavoittuvuuksien tunteminen korostuvat. Haavoittuvuuksien käsittelemiseksi ja uhkaan vastaamiseksi on ohjattava resursseja sekä muodostettava luotettava, yhteiskunnan kaikki toimialueet kattava tilannetietoisuus. Ilman tilannetietoisuutta päätöksentekijöiden on mahdotonta tunnistaa todellista muutosta sekä tehdä oikeita johtopäätöksiä tarvittavista toimenpiteistä. Uhkiin vastaaminen ja niiden torjuminen edellyttää valtioilta strategista valmiutta, joka koostuu kattavasta uhkaympäristön tilannekuvasta, ennakoinnin mahdollistavista elementeistä sekä välineistä poliittisten suositusten ja toimintasuunnitelmien laatimiseen.

Erityishuomiot:

Esityksen uudistuksessa on sinänsä kyse hallinnollisesta muutoksesta, jossa Liikenteen turvallisuusvirasto, Viestintävirasto sekä Liikenneviraston tietyt toiminnot yhdistettäisiin uudeksi virastoksi, Liikenne- ja viestintävirastoksi**.** Näiden virastojen toimintalaajuudesta ja turvallisuustoiminnan kannalta erityisen merkittävästä toiminnasta johtuen muutos on kuitenkin itsessään jo merkittävä.

Esityksen mukaan (sivu 61) turvallisuusvaikutusten osalta tulevaisuudessa äly- ja automaatioliikenne aiheuttavat kyberturvallisuusuhkia, joiden torjunnassa on hyötyä tehokkaammasta yhteistyöstä Kyberturvallisuuskeskuksen kanssa. Euroopan hybridiuhkien torjunnan osaamiskeskus yhtyy tähän kantaan.

2 luku Liikenne- ja viestintäviraston organisaatio ja johtaminen

5 §. Kyberturvallisuuskeskus (sivu 85). Pykälän yksityiskohtaisten perusteluiden mukaan virastossa toimii suoraan pääjohtajan alaisuudessa valtakunnallisista tietoturvallisuustehtävistä vastaava organisatorisesti ja toiminnallisesti erillinen Kyberturvallisuuskeskus. Keskuksen asema perustuisi suoraan tämän lain säännöksiin. Tarkoituksena olisi säilyttää nykyinen Kyberturvallisuuskeskus toiminnallisesti erillisenä, mutta eheänä kokonaisuutenaan myös perustettavassa Liikenne- ja viestintävirastossa. Viraston pääjohtaja ei voisi muuttaa Kyberturvallisuuskeskuksen asemaa 8 §:n nojalla antamallaan viraston työjärjestyksellä. Samoin Kyberturvallisuuskeskuksen toiminnallinen erillisyys muusta Liikenne- ja viestinvirastosta olisi laissa säädetty. Siten keskuksen tai sen osien toimintaa ei voisi hajauttaa perustettavassa virastossa eikä keskuksen osia voitaisi sijoittaa viraston eri toimialoihin tai yksiköihin.

Kyberturvallisuuskeskuksen toiminta tulisi järjestää mahdollisimman ketteräksi ja itsenäiseksi. Erityisesti keskuksen toimintaan liittyvät operatiivisesti käsiteltävät asiat olisi ratkaistava välittömästi. Lisäksi tietoturvaloukkauksia koskevan tiedottamisen ja päätöksenteon olisi oltava nopeaa ja tehokasta. Kyberturvallisuuteen liittyvää tilannejohtamista sekä kansallista ja kansainvälistä koordinointia sekä tiedonvaihtoa ja julkaisuja koskevan päätöksenteon tulisi olla joustavaa ja joutuisaa.

Keskuksen aseman säätämistä organisatorisesti ja toiminnallisesti erilliseksi muusta Liikenne- ja viestintävirastosta puoltaa myös se, että Kyberturvallisuuskeskus on tunnettu ja luotettu yhteistyökumppani useissa kansainvälisissä verkostoissa. Verkostoista saatu tieto ajankohtaisista uhkista ja ilmiöistä on välttämätöntä kansallisen kyberturvallisuuden varmistamisessa. Tietojen puuttuminen heikentäisi kansallista havainnointikykyä ja tilannekuvatuotantokykyä merkittävästi.

Kansainvälisesti on saatu lukuisia esimerkkejä siitä, että hallitsemattomasti toteutetut muutokset kansallisissa tietoturvavastuissa ja niiden organisoinnissa ovat johtaneet luottamusverkostojen ulkopuolelle jättämiseen.

Kyberturvallisuuskeskuksen olisi toimittava poikkihallinnollisesti ja joustavasti. Poikkihallinnollisella toiminnalla tarkoitetaan sitä, että keskuksen olisi jatkettava myös perustettavassa virastossa toimintaansa siten, että se tarjoaa palveluitaan kaikille yhteiskunnan sektoreille. Sen olisi jatkettava yhteistoimintaansa eri viranomaisten ja toimijoiden kanssa. Kyberturvallisuuskeskuksen nykyisiä kansallisia yhteistyötahoja ovat muun muassa sisäministeriö, valtiovarainministeriö, puolustusministeriö, Huoltovarmuuskeskus, Puolustusvoimat ja Rajavartiolaitos.

Joustavalla toiminnalla tarkoitetaan momentissa sitä, että Kyberturvallisuuskeskuksen toiminnan tulisi sopeutua nopeasti sen toimintaympäristössä ilmeneviin häiriöihin, poikkeamiin ja muutoksiin. Keskuksen tulisi myös kyetä ottamaan huomioon yhteiskunnan eri toimijoiden ja sektoreiden erilaiset asiakastarpeet. Kyberturvallisuuskeskuksen luotettavuudesta, toiminnan jatkuvuudesta ja operatiivisista toimintaedellytyksistä pitää huolehtia.

Kyberturvallisuuskeskuksen toiminnassa yhdistyvät erilaiset kansalliset tietoliikenteen turvallisuusviranomaistehtävät ja tietoturvayhteyspisteenä toimiminen, mikä mahdollistaa kansainvälisestikin arvioituna merkittäviä synergiaetuja. Esimerkiksi keskuksen valmistellessa tietoturvasäädöksiä tai valvoessa niiden noudattamista, keskus pystyy hyödyntämään erityistä asiantuntijuuttaan ajankohtaisista tietoturvailmiöistä. Toisaalta keskus pystyy käyttämään viranomaistoimivaltaansa tietoturvauhkilta suojautumiseen ja niiden negatiivisten vaikutusten hillitsemiseen. Nämä ovat myös perusteita, joiden vuoksi Kyberturvallisuuskeskuksen organisatorinen ja toiminnallinen asema esitetään säädettäväksi erilliseksi.

Liikenne- ja viestintäviraston rooli kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaisena turvallisuusviranomaisena (NCSA) kohdistaa Kyberturvallisuuskeskukseen merkittävästi turvallisuusvaatimuksia niin teknisen, henkilöstön kuin fyysisen turvallisuudenkin osalta. NCSA-tehtävien uskottava hoitaminen edellyttää keskuksen riippumatonta ja itsenäistä asemaa, sillä toiminta voi arvioida myös Liikenne- ja viestintäviraston omia tietojärjestelmiä. NCSA-toimintaan ja kansainvälisiin tietoturvallisuusvelvoitteisiin liittyen Kyberturvallisuuskeskuksella on käytössään useita, erittäin korkealle luokiteltuja kansainvälisiä tietojärjestelmiä. Kyseiset järjestelmät ja NCSA-toiminta edellyttävät kansallisten ja kansainvälisten turvallisuusvaatimusten mukaisia turvallisuusjärjestelyjä, joita edellytetään ST III ja ST II - luokitusmerkinnän tiedoille ja kansainvälisten turvallisuuslukitusmerkintöjen EU-C, EU-S, Nato-C ja Nato-S tasoille. EU ja Nato tarkastavat turvallisuusvaatimusten täyttymisen määräajoin. Samat turvallisuusvaatimukset koskevat myös PRS-viranomaisen toimintaa.

Edellä mainittua esitystä Kyberturvallisuuskeskuksen asemasta Euroopan hybridiuhkien torjunnan osaamiskeskus pitää erityisen kannatettavana ja tärkeänä.

1.81 Valtion virkamieslaki 750/1994

Lakiehdotuksen mukaan (sivu 202) uutena asiana virkamieslain 7 §:n mukaan Suomen kansalaisuus vaadittaisiin myös Liikenne- ja viestintäviraston, Väyläviraston sekä Ilmatieteen laitoksen virassa, johon kuuluu tieto- ja kyberturvallisuuteen

olennaisesti vaikuttavia tehtäviä. Liikenne- ja viestintävirastossa kohta koskisi Kyberturvallisuuskeskuksen ja taajuushallinnon virkamiehiä. Viroissa kerääntyy kansallisen turvallisuuden kannalta merkittävää tietoa, joita käytetään päätöksenteon tueksi. Lisäksi viroissa on myös mahdollisuus vaikuttaa valtionhallinnon ja turvallisuusviranomaisten sekä muutenkin kansallisen turvallisuuden kannalta keskeisten verkkopalveluiden kyberturvallisuuteen.

Kyberturvallisuuskeskus toimii kansallisena tietoliikenneturvallisuusviranomaisena (NCSA, National Communications Security Authority), joka vastaa turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioista. Toiminto on osa Suomen turvallisuusviranomaisorganisaatiota. Toiminnon tehtäväkokonaisuudet liittyvät kansainvälisiin ja kansallisiin turvallisuusvelvoitteisiin. Niiden tärkeimpänä tarkoituksena on suojata toisen valtion suomalaiselle toimijalle luovuttamaa salassa pidettävää tietoa tai suomalaisen viran- omaisen salassa pidettävää tietoa, kun sitä luovutetaan yrityksille. Lisäksi toiminta edistää turvallisuutta sekä viranomaisissa että yrityksissä.

Edellä mainittua esitystä Euroopan hybridiuhkien torjunnan osaamiskeskus pitää myös erityisen kannatettavana ja tärkeänä.

Lopuksi: Edellä mainittujen turvallisuusympäristön muutoksiin liittyvien syiden perusteella Euroopan hybridiuhkien torjunnan osaamiskeskus katsoo otsikossa mainitun esityksen olevan omalta osaltaan kannatettava ja perusteltu.

.