9.5.2022

Eduskunta
Liikenne- ja viestintävaliokunta

HE 63/2022 vp Hallituksen esitys eduskunnalle laeiksi valmiuslain ja asevelvollisuuslain 79 §:n muuttamisesta / Asiantuntijapyyntö

## Lausunto: Valmiuslain ja asevelvollisuuslain 79 §:n muuttaminen

Finnish Information Security Cluster – Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyber- ja tietoturvallisuusalaa. Tässä lausunnossa huomio kohdistetaan erityisesti *digitaaliseen toimintaympäristöön (ml. tietoliikenne)*.

Kyberala kannattaa esityksen tavoitteita. Pidämme tärkeänä, että esityksessä kuvatuissa monimutkaisissa ja monialaisissa sekä nopeasti muuttuvissa hybridivaikuttamisen tilanteissa viranomaisten toimivaltuudet ovat riittävät, normaalivaltuuksista poikkeavien valtuuksien käyttöönotto onnistuu tarvittaessa nopeasti ja säännökset ovat myös tulkinnallisesti selkeitä.

Kyberala kannattaa pääosin ehdotettua lisäystä poikkeusolojen määritelmään (3 § 6)-kohta) sekä sen perusteita. Digitaalisen ympäristön sekä sen kytkeytymisen potentiaalisiin reaalimaailman seurauksiin, on tärkeää, että määritelmässä on pyritty huomioimaan myös yhtäaikaisten toimien vaikutus. Kiinnitämme kuitenkin huomiota joihinkin esityksen kohtiin seuraavasti:

**Esitetty hybridivaikuttamiseen liittyvä poikkeusolojen määritelmä ja sen perusteet**

Esityksessä (s. 41, kolmannen kappaleen viimeinen virke) todetaan: ”Myös kriittisen infrastruktuurin toimintaan kohdennettavalla verkkohyökkäyksellä uhkaamista voitaisiin pitää säännöksessä tarkoitettuna uhkana, jos se olisi mittakaavaltaan ja vaikutuksiltaan riittävän vakava.” Kyberala haluaa painottaa, että koska vakavillakin toimilla tai seurauksilla uhkaamista on helppoa harjoittaa, **uhkaamisen osalta on edellytettävä, että se on vakavasti otettavaa erityisesti uhkaajan tahtotilan, aikomusten, kyvykkyyden, keinovalikoiman, pidäkkeiden sekä vastaanottajan haavoittuvuuden näkökulmasta**. Pelkästään sitä, että on esitetty verkkohyökkäykseen liittyvä vakavakin uhkaus, ei yksinään voi pitää riittävänä.

Asiassa tulisi huomioida myös se, että kaikissa tapauksissa ei todennäköisesti olisi mahdollisuutta jälkikäteenkään todentaa, mistä syystä tai minkä tahon toimesta hyökkäys on aiheutunut. Kun poikkeusolojen toteaminen on kuitenkin voitava objektiivisten ja havaittavien seikkojen pohjalta todeta, on perusteltua keskittyä siihen, mihin uhka tai toiminta kohdentuu ja mitkä sen vaikutukset ovat tai olisivat.

Lisäksi **tulisi muutoinkin harkita, onko perustelutekstissä tarpeen säilyttää ko. uhkauksen olemassaoloa säännöksessä tarkoitettuna uhkana**. Lisäharkinnan perusteita ovat myös mm. se, mitä ”uhkaamisella” tarkoitetaan. Olisiko kyse nimenomaan jonkin valtion tai valtiollisen toimijan toiminnasta, ja olisiko kyse vain jonkin vakavan häiriön laukaisemisen (esim. jo levitetyn kyberaseen aktivoiminen) uhkaamisesta, vai yleisemmin eksplisiittisestä, sanoin ilmaistusta *uhkauksesta*, vai myöskin implisiittisestä *uhan* muodostamisesta ja siihen


Eteläranta 10, PL 10, 00131 Helsinki
www.fisc.fi

liittyvistä valmistelutoimista ja muista esim. turvallisuustiedustelun tai rikostutkinnan kautta saatavista tiedoista.

Vaikka onkin selvää, että laaja-alainen määrittely on yleisesti ottaen perusteltua tarkoitustaan vastaan helposti kääntyvä liian ahtaan tulkinnan vuoksi, Kyberala kehottaa harkitsemaan perustelutekstin varsin suppeaa ja osin perustelematonta uhkaukseen perustuvaa kohtaa valmiuslain poikkeusolojen toteamisen perusteena ja kysyy, rikkoisiko toteamiskynnys perusoikeussuojaa ja sen vakiintunutta ydinsisältöä (perustuslain 23 §:ssä tarkoitetuista kansakuntaa uhkaaviin poikkeusoloista, jotka kiinnittyvät kansainvälisten ihmisoikeussopimusten mukaiseen yleisen hätätilan käsitteeseen ja joissa on kyse vakavasta uhasta kansakunnan elämälle ja olemassa- ololle)?

Perusteluissa (s. 44, ensimmäinen virke) todetaan, että ”Ehdotetussa poikkeusolomääritelmässä tarkoitetut uhkat voisivat siten johtua myös ihmisten tahattomasta toiminnasta.” Kyberala pitää kuitenkin selvää, että **jos kyse on ihmisten tahattomasta toiminnasta ja tämä voidaan riittävällä varmuudella todeta, sen tulisi nostaa poikkeusolojen toteamisen kynnystä 3 §:n 6)-kohdan perusteella**.

**<u>Käyttöön otettavat toimivaltuudet valmiuslain 3 § 6)-kohdassa tarkoitetuissa poikkeusoloissa</u>**

Kyberala pitää tärkeänä ja kannatamme myös sitä esityksessä omaksuttua valintaa, että uuden valmiuslain 3 §:n 6)-kohdan määritelmän täyttyessä voitaisiin poikkeusolojen toimivaltuuksia ottaa käyttöön vain rajatusti ja kunkin yksittäisen toimivaltuussäännöksen osalta luonnollisesti välttämättömyys- ja oikeasuhtaisuusvaatimukset huomioiden. Koska poikkeusoloperusteen määrittely täysin tyhjentävästi ja tarkkarajaisesti on joka tapauksessa varsin haastavaa erityisesti hybridivaikuttamista koskevissa monimutkaisissa tilanteissa, tärkeää on, että käyttöönottoasetusten normaali kontrollimekanismi on käytössä ja tarjoaa mahdollisuuden vielä arvioida tilanne ja kriteerien täyttyminen eduskunnassa.

**<u>Viestintäverkkoihin ja viestintäpalveluihin kohdistuvat toimenpiteet</u>**

Kyberalan näkökulmasta esityksessä jää epäselväksi miltä osin, jos ollenkaan, viestintäverkkoihin ja palveluihin kohdistuvien toimenpiteet ulottuvat varsinaisten teleyritysten ulkopuolisiin toimijoihin, mm. kolmanteen sektoriin.

Lakiehdotuksen 60 §:n mukaan ”*Sähköisten tieto- ja viestintäjärjestelmientoimivuuden turvaamiseksi ja niihin kohdistuvien tietoturvauhkien torjumiseksi liikenne- ja viestintäministeriö voi 3 §:n 1–3 ja 6 kohdassa tarkoitetuissa poikkeusoloissa päätöksellään velvoittaa sähköisen viestinnän palveluista annetussa laissa (917/2014) tarkoitetun teleyrityksen…*”

Sähköisen viestinnän palveluista annetun lain (917/2014), 1 luvun 3 §:n 27)-kohdassa teleyrityksellä tarkoitetaan sitä, joka tarjoaa verkkopalvelua tai viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille eli harjoittaa yleistä teletoimintaa. Kuitenkin Suomessa, kuten muuallakin Euroopassa, osa tietoverkkojen hallintaan liittyvästä kriittisestä infrasta on kolmannen sektorin hallinnoimaa, konkreettisena esimerkkinä Internetin juurinimipalvelimet manner-Suomen alueella.


Eteläranta 10, PL 10, 00131 Helsinki
www.fisc.fi

Näin ollen Kyberala pyytää arvioimaan**, tulisiko ainakin valmiuslain 60 §:n soveltamisalaa laajentaa kattamaan myös ko. toimijakenttä ja tarkentaa ehdotuksessa onko, ja millä oikeusperustalla olisi mahdollista ulottaa velvoitteita myös muille kuin teleyrityksille**.

**Lopuksi**

Kyberala kiittää siitä, että esitykseen sisältyvät muutostarpeet päätettiin viedä läpi nopeutetussa menettelyssä riippumatta siitä, että Oikeusministeriö oli jo ennen niiden valmistelun aloittamista, joulukuussa 2021 päättänyt aloittaa valmiuslain kokonaisuudistuksen.

**Kannatamme edelleen kokonaisuudistuksen käynnistämistä ja käsillä oleva tilanne huomioiden, sen kiirehtimistä**. Myös valmiuslainsäädäntöä uudistettaessa on pyrittävä hyödyntämään koronakriisin opit. Kriisin alkaessa keväällä 2020 oli käsitys, että lainsäädäntömme oli kunnossa. Nopeasti kävi kuitenkin selväksi, että näin ei ollut. Tässä esityksessä huomioitu ns. muuttoliikkeen esineellistäminen, ts. välineellistetty maahantulo on toinen esimerkki opitusta; ennen vuotta 2015 ei ajateltu, että valmiuslainsäädännön tulisi vastata tällaiseen tilanteeseen.

Kyberala katsoo, että mikäli kyseisellä menettelyllä, tai millä tahansa vaikeasti tunnistettavalla keinolla heikennetään vakavasti ja laajamittaisesti valtiovallan (ml. keskeiset viranomaistoiminnot) kykyä turvata yhteiskunnan jäsenten perusoikeudet ja -vapaudet, tai perusturvallisuus reaali- tai digitaalisessa ympäristössä**, valmiuslain on kyettävä tarjoamaan riittävät toimivaltuudet**. Esimerkiksi kansainvälisten sopimusten turvapaikkaa koskeva oikeus edellyttää, että turvapaikanhakijalla on perusteltu syy pelätä joutuvansa vainon eli perustavanlaatuisten ihmisoikeusloukkausten kohteeksi lähtömaassaan. Tämän oikeuden kaikenlainen väärinkäyttö esim. väliintulijavaltion toimesta ei kuulu sopimusten tarkoituksiin. Mikäli jokin valtio toteuttaa järjestelmällistä sopimuksen tarkoituksen ulkopuolista – jopa vastaista – toimintaa ei Suomen tule olla sidottu kantamaan vastuuta turvapaikkaoikeuden toteuttamisesta. Tällaisessa tilanteessa kansallinen turvallisuuden, yhteiskunnan toimintakyvyn ja väestön elinmahdollisuuksien turvaaminen on ensisijaista.

Nämä havainnot alleviivaavat sitä, että valmiuslainsäädännön uudistamisen pohjaksi tulee laajapohjaisessa yhteistyössä kehittää erilaisia kriisiskenaarioita riittävän pitkälle, jotta tunnistettaisiin, millaisiin tilanteisiin lainsäädännön tulisi vastata. Elinkeinoelämän tulee olla mukana tässä valmistelutyössä, sillä kaikki kansallista turvallisuutta ja yhteiskunnan toimintakykyä vaarantavat toimet heijastuvat myös elinkeinoelämään ja sen kykyyn huolehtia tehtävistään yhteiskunnan resilienssin varmistamisessa.

Näin toimien löydetään yhteistyössä mahdollisimman kattavasti ne tarpeet, joihin lainsäädännön kokonaisuutena tulee vastata. Osa näistä ratkaistaan valmiuslainsäädännön keinoin, mutta merkittävä osa ratkaistaan kehittämällä normaaliaikojen toimivaltuuksiin liittyvää lainsäädäntöä, koska **valmiuslainsäädännön käyttökynnyksen tulee jatkossakin olla korkea.** Tästä syystä muutostarpeita tunnistettaessa ei ole riittävää pohtia skenaarioita vain poikkeusolojen määritelmästä lähtien.

Lisätiedot:

Toimitusjohtaja, Peter Sund
sähköposti: peter.sund@teknlogiateollisuus.fi
puhelin: 050 565 0621



Eteläranta 10, PL 10, 00131 Helsinki
www.fisc.fi