

Hallintovaliokunta
hav@eduskunta.fi

Viite
Asiantuntijapyyntönnö, HE 63/2022 vp

Liikenne- ja viestintäviraston kyberturvallisuuskeskuksen lausunto hallituksen esitykseen eduskunnalle laeiksi valmiuslain ja asevelvollisuuslain 79 §:n muuttamisesta

Hallintovaliokunta on pyytänyt asiantuntijaa kuultavaksi ja kirjallista asiantuntijalausuntoa hallituksen esityksestä eduskunnalle laeiksi valmiuslain ja asevelvollisuuslain 79 §:n muuttamisesta, HE 63/2022 vp.

Liikenne- ja viestintäviraston kyberturvallisuuskeskus kiittää mahdollisuudesta lausua asiassa. Keskus keskittyy lausunnossaan erityisesti sen omaa toimialaa koskevien ehdotusten arviointiin.

Hybridiuhat

Kyberturvallisuuskeskus pitää erittäin kannatettavana valmiuslain muuttamista siten, että poikkeusolojen määritelmä kattaisi myös hybridiuhat. Esitys vastaa Suomen turvallisuustilanteessa tapahtuneisiin muutoksiin ja erityisesti lisääntyneeseen hybridi vaikuttamiseen. Uusi poikkeusolojen määritelmä mahdollistaisi puuttumisen tilanteisiin, jotka eivät yksin riitä täyttämään voimassaolevan lain poikkeusolojen määritelmää.

Valmiuslaki mahdollistaa jo nykyisellään tietyssä määrin puuttumisen myös hybridi vaikuttamiseen. Esityksessä viitataan esimerkkinä aseelliseen hyökkäykseen vakavuudeltaan rinnastuvaan tietojärjestelmiin kohdistuvaan iskuun. Hybridi vaikuttamisen tilanteessa ongelmaksi voi kuitenkin muodostua se, ettei tilannetta välttämättä pystytä määrittämään varsinaisesti hyökkäykseksi. Hybridi vaikuttamiseen tyypillisesti liittyy tarkoituksellista tilanteen luonteen ja alkuperän hämärtämistä. Valmiuslain 3 §:n 1 ja 2 kohdan säännökset eivät esityksessä todetun mukaisesti myöskään ota huomioon erilaisten vaikuttamiskeinojen yhteisvaikutusta. Siten on ensiarvoisen tärkeää, että valmiuslain poikkeusoloja koskevaa määritelmää tarkistetaan siten, että se vastaa erityisen vakaviin ja monimuotoisiin hybridi vaikuttamistilanteisiin.

Kriittinen infrastruktuuri

Kyberturvallisuuskeskus pitää hyvänä, että kriittisen infrastruktuurin määrittämisessä otetaan huomioon valtioneuvoston päätöksen huoltovarmuuden tavoitteista (1048/2018) sisältyvä kriittisen infrastruktuurin määritelmä, johon luetaan mukaan mm. digitaalisen yhteiskunnan tietojärjestelmät sekä viestintäverkot ja -palvelut. Näiden käytettävyydestä, luottamuksellisuudesta ja eheydestä eli tietoturvan eri osa-alueista huolehtiminen on tärkeää mahdollisissa hybridiuhkatilanteissa.

Toimivaltuudet

Laissa säädettäisiin myös niistä toimivaltuuksista, joita viranomaisille olisi mahdollista antaa uuden poikkeusolomääritelmän mukaisesti todetuissa poikkeusoloissa. Esitys mahdollistaa toteutuessaan viranomaisten mahdollisuudet puuttua tehokkaasti vallitsevan yhteiskunnallisen tilanteen mukaisiin turvallisuusuhkiin.

Kuten esityksessä on tuotu esiin, Liikenne- ja viestintävirastolla ja sen Kyberturvallisuuskeskuksella on jo normaaliolojen lainsäädännön puitteissa laajat toimivaltuudet puuttua erilaisiin sähköisen viestinnän palvelujen häiriötilanteisiin. Esityksessä todetun mukaisesti normaalioloja koskevalla sääntelyllä ei kuitenkaan ole mahdollista vastata hybridi-vaikuttamisen kaikista vakavimpiin muotoihin, minkä vuoksi on hyvä, että esityksessä on tarkasteltu myös viranomaisten toimivaltuuksia hybridi-vaikuttamisen näkökulmasta.

Kyberturvallisuuskeskus pitää hyvänä ehdotusta, jonka mukaan hybridi-vaikuttamista koskevissa, valmiuslain 3 §:n 6 kohdan mukaisissa poikkeusoloissa mahdollistettaisiin sähköisten tieto- ja viestintäjärjestelmien toimivuuden turvaamista koskevan valmiuslain 9 luvun toimivaltuuksien soveltaminen, sillä näiden säännösten tavoitteena on ylläpitää poikkeusoloissa yhteiskunnan toiminnan kannalta elintärkeiden tieto- ja viestintäjärjestelmien toimintaa.

Kyberturvallisuuskeskus pitää myös hyvänä, että uudistuksessa huomioidaan hallinnonalan virastouudistus niin, että laista käy selvästi esille nykyisten virastojen vastuut.

Palvelussuhteen ehdoista poikkeaminen ja irtisanomisoikeuden rajoittaminen

Kyberturvallisuuskeskus pitää hyvänä ehdotusta, jonka mukaan Kyberturvallisuuskeskus itse ja Liikenne- ja viestintäviraston taajuushallinto sisältyisivät valmiuslain 93.2 §:ään ja 94.4 §:ään. Virasto hoitaa yhteiskunnan toiminnan ja turvallisuuden sekä sotilaallisen koskemattomuuden kannalta kriittisiä tehtäviä, jotka tulee turvata myös valmiuslain ehdotetun 3 §:n 6 kohdan mukaisissa poikkeusoloissa.

Kyberturvallisuuskeskus hoitaa useita yhteiskunnan toimivuuden ja turvallisuuden kannalta keskeisiä tehtäviä ja näin ollen mahdollisissa hybridiuhkatilanteissakin keskeistä on riittävien henkilöstöresurssien varmistaminen:

- Kyberturvallisuuskeskus huolehtii viestintätoimialan, ml. teleyritysten tarjoamien yleisten viestintäverkkojen ja -palvelujen varautumisesta normaaliolojen häiriötilanteisiin ja poikkeusoloihin, edistää ja valvoo sähköisen viestinnän toimintavarmuutta, tietoturvaa ja luottamuksellisen viestinnän suojan toteuttamista sekä tukee toimialallaan yhteiskunnan yleistä varautumista normaaliolojen häiriötilanteisiin ja poikkeusoloihin.
- Kyberturvallisuuskeskus kerää ja jakaa hybridipoikkeusolojenkin kannalta ensiarvoisen tärkeää kyberturvallisuuden yhdistettyä tilannekuvaa päätöksenteon tueksi. Kyberturvallisuuskeskuksen tilannekuvatuotanto osaltaan mahdollistaa poikkeusoloissa valtioneuvoston kyvyn tehdä tarkempia lisäpäättöksiä valmiuslain käytön tarpeesta.
- Keskus auttaa kyberhyökkäysten ennalta ehkäisyssä ja niistä toipumisessa.
- Kansainvälisistä tietoturvallisuusvelvoitteista, turvallisuusselvityksistä sekä viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista annettujen lakien mukaan Kyberturvallisuuskeskukselle kuuluvat erilaiset tietojärjestelmien turvallisuusarvioinnit ja -hyväksynät.
- Kansainvälisen turvaluokitellun tiedon osalta Kyberturvallisuuskeskus toimii kansallisena turvallisuusjärjestelyjen hyväksyntäviranomaisena, salaustuotteiden, sekä salatun aineiston jakelusta vastaavana viranomaisena.
- Kyberturvallisuuskeskus on salausteknisen materiaalin jakelusta vastaava viranomainen. Kyberturvallisuuskeskus hallinnoi salausteknisen materiaalin jakeluverkkoa, vastaa jakelusta ja ohjeistaa sen turvalliseen käsittelyyn. Jakeluverkko koostuu turvallisuusviranomaisista ja ministeriöistä.
- Kyberturvallisuuskeskus toimii julkisesti säännellyn satelliittipalvelun vastuuviranomaisena (PRS Galileo) ja Euroopan kyberturvallisuuden teollisuus-, tekno-

logia- ja tutkimusosaamiskeskuksen ja kansallisten koordinoitavien verkostojen perustamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2021/887 6 artiklan mukaisena kansallisena koordinoitavien keskuksena.

Kyberturvallisuuskeskuksen toiminnalla siis varmistetaan, että yleisten viestintäverkkojen ja -palvelujen varaan rakentuvat yhteiskunnan digitaaliset palvelut ovat luotettavasti käytettävissä normaalioloissa ja myös valmiuslain mukaisissa poikkeusoloissa. On huomioitava, että ehdotetun valmiuslain 3 §:n 6 kohdan kuvaamissa oloissa digitaalinen yhteiskunta toimii vielä varsin normaalisti ja Kyberturvallisuuskeskus tuottaisi korotetun valmiuden vaatimia palveluitaan muun muassa kriittisen infrastruktuurin toimijoille. Kaikissa poikkeusoloissa kyberhäiriöt voivat vaikuttaa laajasti muun muassa terveydenhuoltoon, liittyä suuronnettomuuksiin ja ne ovat tyypillisesti keskeinen hybridi-vaikuttamisen menetelmä.

Kyberturvallisuuden asiantuntijoita, esimerkiksi salausteknisen materiaalin hallintointia hoitavia henkilöitä, ei ole tehtävien edellyttämän kokemuksen ja osaamisen vuoksi mahdollista korvata muilla henkilöillä. Poikkeusoloissa kriittisten henkilöiden vähäinen määrä huomioon ottaen työaika-rajat täyttyvät nopeasti. Näin ollen, jotta Kyberturvallisuuskeskus voi varmistaa keskeytymättömän toimintansa, sillä tulee olla mahdollisuus poiketa palvelussuhteen lepoaikoja, ylityötä ja vuosilomaa koskevista ehdoista myös valmiuslain 3 §:n 4 ja 5 sekä 6 kohdan tarkoittamissa tilanteissa. Samoin on välttämätöntä mahdollistaa Kyberturvallisuuskeskuksen henkilöstöön kohdistuvan irtisanomisoikeuden rajoittaminen 3 §:n 4 ja 5 sekä 6 kohdassa tarkoitetuissa poikkeusoloissa, jotta voidaan varmistaa kriittisten henkilöstöresurssien pysyvyys mahdollisissa taloudellisissa poikkeustilanteissa.