



13.5.2020

## Lausuntokooste luonnoksesta valtioneuvoston asetukseksi julkisen hallinnon turvallisuusverkko toiminnasta annetun valtioneuvoston asetuksen muuttamisesta

Julkisen hallinnon turvallisuusverkko toiminnasta annetun lain (10/2015) muutoksella (53/2019) säädettiin viranomaisradioverkon (VIRVE:n) sekä viranomaisten aikakriittisen laajakaistaisen matkaviestinnän tieto- ja viestintä teknisten palvelujen tuotannosta turvallisuusverkkolain mukaisina palveluina.

Ehdotetulla valtioneuvoston asetuksella on tarkoitus tehdä julkisen hallinnon turvallisuusverkko toiminnasta annettu valtioneuvoston asetukseen (1109/2015) mainitusta lain muutoksesta johtuvat muutokset sekä muutamia muita vähäisiä tarkistuksia.

### 1 Lausuntopyyntö, jakelu ja lausunnon antaneet

Asetusluonnos oli lausuntokierroksella 24.3. – 30.4.2020. Lausuntopyynnön jakelussa olivat ministeriöt, Tasavallan presidentin kanslia Digi- ja väestötietovirasto, Elinkeinoelämän keskusliitto, Huoltovarmuuskeskus, Suomen Erillisverkot Oy, Suomen Kuntaliitto, Tietoliikenteen ja tietotekniikan keskusliitto, FiCom ry ja Valtion tieto- ja viestintätekniikkakeskus Valtori.

Jakelussa mainittuja ministeriöitä pyydettiin kokoamaan hallinnonalan TUVE-käyttäjätahojen lausunnot. Sisäministeriötä pyydettiin kokoamaan lisäksi pelastuslaitosten lausunnot. Sosiaali- ja terveysministeriötä pyydettiin kokoamaan sairaanhoitopiirien ja ensihoidosta vastaavien lausunnot. Valtiovarainministeriön KHT-osastoa pyydettiin kokoamaan muiden kuin jakelussa mainittujen VM:n hallinnonalan TUVE-käyttäjien lausunnot.

Lausuntoja saatiin yhteensä 20 kappaletta. Lausuntonsa toimittivat:

Digi- ja väestötietovirasto (ei lausuttavaa)  
Elinkeinoelämän keskusliitto (ei lausuttavaa)  
Elisa Oyj

Kilpailu- ja kuluttajavirasto

Seuraavat pelastuslaitokset (SM:n lausunnon yhteydessä)

- Helsingin kaupungin pelastuslaitos
- Itä-Uudenmaan pelastuslaitos
- Keski-Pohjanmaan ja Pietarsaaren alueen pelastuslaitos
- Länsi-Uudenmaan pelastuslaitos
- Oulu-Koillismaan pelastusliikelaitos
- Pohjanmaan pelastuslaitos
- Satakunnan pelastuslaitos
- Varsinais-Suomen pelastuslaitos

Puolustusministeriö

Sisäministeriö

Sosiaali- ja terveysministeriö (ei lausuttavaa)

Suomen Erillisverkot Oy

Säteilyturvakeskus (ei lausuttavaa)  
 Tasavallan presidentin kanslia (ei lausuttavaa)  
 Ulkoministeriö  
 Valtion tieto- ja viestintätekniikkakeskus Valtori

## 2 Yhteenveto lausunnoista

Yleisvaikutelma lausunnoista on, että ehdotetut asetuksen muutokset nähdään tarpeellisena. Palvelutuottajien vastuunjaon selkeyttä ja toisaalta yhteistoimintaa palvelutuotannossa korostettiin. Myös varautumisen ja tietoturvallisuuden vaatimuksiin esitettiin kehitysehdotuksia. Turvallisuusverkon palvelujen käyttöä koskevan sääntelyn muutos nähtiin pääosin positiivisena, mutta toisaalta uusia käyttäjäorganisaation tietoturvallisuutta koskevia vaatimuksia osin kritisoitiin.

Lausunnoissa olleet yksityiskohtaisemmat kommentit on ryhmitelty seuraavasti:

- Tieto- ja viestintätekniisten palvelujen tuottajan tehtävät ja palvelut (3 §)
- Varautuminen (8 §)
- Tietoturvallisuusvaatimukset (9 §)
- Turvallisuusverkon palvelujen käyttö (11 §)
- Muut asiat

### 2.1 Tieto- ja viestintätekniisten palvelujen tuottajan tehtävät ja palvelut (3 §)

Suomen Erillisverkot Oy:n (ERVE) mukaan asetuksen uudessa 3 momentissa luetellut tehtävät ja palvelut eivät kata kaikkia Virve 2.0- palveluiden tuottamisen osa-alueita. Esimerkiksi Virve 2.0 -palveluiden tarjoamiseksi, tarvitaan kriittisen palvelujen tuottamiseen mobiilipalvelualusta, joka sisältää myös esim. "geneerisen reunalaskentapalvelun", jota tarjotaan myös asiakkaille.

ERVE esitti luonnoksen 3 § 3 momentin kohtaa

*5) viranomaisten aikakriittisen laajakaistaisen matkaviestinnän liittymät muutettavaksi muotoon liittymäpalvelut, koska kaikki muutkin kohdat ovat palveluja.*

Lisäksi ERVE esitti lisättäväksi uudet kohdat 7) -10) ja olevat kohdat 7) ja 8) muutettaviksi ja uudelleennumeroitaviksi seuraavasti:

*"Turvallisuusverkkolain 9 §:n 2 momentin 1 kohdassa tarkoitettuja viranomaisradioverkon sekä viranomaisten aikakriittisen laajakaistaisen matkaviestinnän yhteisiä tieto- ja viestintätekniisiä palveluja ovat:*

- 1) päätelaittepalvelut;*
- 2) käyttäjätukipalvelut;*
- 3) viranomaisradioverkon liittymäpalvelut;*
- 4) viranomaisradioverkon viestintätekniiset palvelut;*
- 5) viranomaisten aikakriittisen laajakaistaisen matkaviestinnän liittymäpalvelut;*
- 6) viranomaisten aikakriittisen laajakaistaisen matkaviestinnän viestintätekniiset palvelut;*
- 7) muut kuin 2 §:ssä tarkoitetut tietoliikennepalvelut;*
- 8) käyttöpalvelut;*
- 9) tietokanta- ja sovellusalustapalvelut;*
- 10) integraatio- ja sanomanvälityspalvelut*
- 11) 1 - 10 kohdassa mainittuihin palveluihin liittyvät tietoturvallisuuspalvelut;*
- 12) 1 - 11 kohdassa mainittuihin palveluihin liittyvät omaisuudenhallintapalvelut."*

ERVE esitti myös, että perustelumuiotiossa todettaisiin 3 § 3 momentissa määriteltyjen Virve 2.0 -palvelujen tarkentuvan hankkeen edetessä. Muistiossa voisi tuoda esille esimerkkejä, millaisia asioita palveluluettelossa mainitut palvelut voivat sisältää. Osa palveluista voi olla myös nykyisiä Virven palveluja.

*"1. Päätelaitepalvelut kuten etähallintapalvelut, elinkaari palvelut, laitteiden omistus (rahoitus ja leasing), tietoturva, mobiili hallinnointipalvelu tai sovellusten kehittäminen*

*2. Käyttäjätukipalvelut kuten palvelun suunnittelu ja käyttöönotto, pääkäyttäjä-palvelu, hallinnointipalvelu, viestiliikenteen tallennuspalvelu tai testauspalvelut*

*3. Viranomaisradioverkon liittymäpalvelut kuten radiopäätelaiteliittymä tai kiinteä päätelaiteliittymä*

*4. Viranomaisradioverkon viestintätekniset palvelut kuten ryhmäpuhelut, yksilöpuhelut, sanomapalvelut, paikannus, suorakanavatoiminto, datapalvelut ja kiinteä liittymä*

*5. Viranomaisten aikakriittisen laajakaistaisen matkaviestinnän liittymäpalvelut kuten viranomaisliittymät, joiden kautta liitytään viranomaisten etuoikeustointeilla varustettuihin toimintokriittisiin laajakaistaisiin matkaviestinnän palveluihin, IoT-liittymät, kiinteät päätelaiteliittymät (IP liittymä), aika- ja synkronointipalvelut (esim. PRS) tai tilannekuvapalvelut*

*6. Viranomaisten aikakriittisen laajakaistaisen matkaviestinnän viestintätekniset palvelut kuten ryhmäpuhelut, yksilöpuhelut, sanomapalvelut, paikannus, suorakanavatoiminto, datapalvelut (SDS ja IP) video, toimintokriittiset mobiilit viestintäpalvelut, paikkatietopalvelut ja niiden hallinta, laitteiden, sensoreiden sekä autonomisten laitteiden kommunikaatio*

*7) Muut kuin 2 S:ssä tarkoitetut tietoliikennepalvelut kuten Reunalaskennan tarvitsemat tietoliikennepalvelut*

*8) Käyttöpalvelut kuten konesalipalvelut, kapasiteettipalvelut, palvelinalustapalvelu, tallennustilapalvelu, varmistuspalvelu, laitepaikkapalvelu, virtualisointipalvelut*

*9) tietokanta- ja sovellusalustapalvelut kuten sovellusten käyttämät tietokantapalvelut, tekoälyn tarvitsemat laskentapalvelut, tekoälyn tarvitsemat tietoallas-palvelut sekä SaaS-, IaaS-, PaaS- ja FaaS-palvelut*

*10) Integraatio- ja sanomavälityspalvelut kuten EAI-palvelut*

*11) 1 - 10 kohdassa mainittuihin palveluihin liittyvät tietoturvasuoypalvelut kuten palomuuripalvelut, hyökkäyksenestopalvelut ja näihin liittyvät raportointipalvelut*

*12) 1 -11 kohdassa mainittuihin palveluihin liittyvät omaisuudenhallintapalvelut kuten laiterekisteripalvelut, lisenssirekisteripalvelut, lisenssien hallintapalvelut, lisenssien, laitteiden ja palveluiden omistaminen ja rahoitus."*

Valtori totesi, että keskeistä on asetuksessa selkeyttää viranomaisverkon tuottamisvastuu ja siihen kuuluvat tehtävät. Tämä selkeyttää Valtorin ja ERVEN tehtävänjakoa. Päätelaitepalvelujen ja käyttäjätukipalvelujen eriyttäminen omiksi kokonaisuuksikseen on luontevaa, koska päätelaitepalvelut pitävät sisällään paljon päätelaitteiden elinkaaranhallintaan liittyviä palveluita ja taas käyttäjätukipalvelut enemmän sitä, kuinka loppukäyttäjien kaikkien palvelujen, ei ainoastaan päätelaitteiden käyttöä, voidaan tukea mahdollisimman hyvin.

Myös Elisa Oyj korosti, että palvelujen tuottamisen turvaamiseksi on erityisen tärkeää, että palvelutuottajien roolit ja näiden vastuulle kuuluvat palvelut on jaettu ja määritelty siten, että niistä muodostuu ehyt kokonaisuus ja että jako on selvä palvelutuottajille, käyttäjille sekä palvelutuotantoon osallistuville alihankkijoille. Kun kyseessä on yhteiskunnan toimivuuden kannalta kriittiset palvelut, tulee pyrkiä hallinnollisesti suoraviivaisiin rakenteisiin, jotta palvelujen tuottaminen pystytään varmistamaan tehokkaasti kaikissa tilanteissa. Tämä korostuu erityisesti valmius- ja varautumistilanteissa. Elisa Oyj:n näkemyksen mukaan asetuksessa tulee selvästi säätää, että kaikki ne tausta- ja muut liitännäispalvelut (kuten sovelluspalvelut ja palvelimet) – jotka liittyvät keskeisesti

pykälän perusteella jommankumman palvelutuottajan vastuulle kuuluviin palveluihin, tulisi olla myös tämän saman toimijan hallinnassa ja vastuulla. Esimerkiksi, mikäli ERVE tarvitsee sen vastuulle kuuluvien mobiilipalvelujen tuottamiseen liittyviä erilaisia taustasovelluksia, kuten liittymien hallintaan tarvittavia palveluja tai muita sovelluspalveluja – tulee tällaisten palvelujen tuottaminen olla selvästi ERVEN hallinnassa ja vastuulla. Mikäli näin ei olisi, on riskinä, että palvelujen tuottaminen ja niiden toiminnan varmistaminen vaarantuu, kun kriittiset palvelurakenteet pirstaloituvat. Elisa Oyj:n mukaan tätä asiaa ei ole riittävästi asetuksessa huomioitu. Palvelutuotannon varmistamisen toteuttamisen kannalta on tärkeää, että Suomen ERVELLÄ on kriittisten palvelujen osalta hallinnollisesti, toiminnallisesti ja teknisesti itsenäinen toimintakyky kaikissa varautumisen ja valmiuden tilanteissa.

Valtorin mukaan nykyisen asetuksen varsin monisanainen tietoturvaluutta koskeva kohta 6 tulisi korvata siten, että kaikissa tuotettavissa palveluissa tulee olla riittävät tietoturvan varmistavat palvelut.

Sisäministeriö (SM) kiinnitti huomiota siihen, että 3 §:ssä käytetään sekä termiä tietoturvapalvelut että termiä tietoturvaluuspalvelut – ja esitti termien yhtenäistämistä, ellei niillä tosiasiallisesti tarkoiteta eri asioita.

SM:n mukaan turvallisuusverkkolain tarkoitus ja samalla koko TUVE-toiminnan ydin on varmistaa turvallisuusverkon käyttäjille yhteisten TUVE-palvelujen häiriöttömyys ja jatkuvuus sekä päätöksenteossa ja johtamisessa tarvittavien tietojen käytettävyyden, eheys ja luottamuksellisuus. Turvallisuusverkkotoimintaa koskevan lainsäädännön tulee tukea käyttäjien lakisääteisistä toimintaa varten tarvitsemien palvelujen saatavuutta, velvoittaa palvelutuottajia tuottamaan käyttäjien tarvitsemat yhteiset palvelut ja valtiovarainministeriötä vastaamaan ohjauksesta ja valvonnasta. Niin palvelujen kuin vastuidenkin on oltava riittävästi selkeitä, täsmällisiä ja tarkkarajaisia, jotta kaikki turvallisuusverkkotoimintaan lakisääteisesti osallistuvat voivat luottaa kaikissa olosuhteissa niin omaan kuin muidenkin toimintaan. Nyt esitettävät muutokset eivät täysin esitettyssä asetuseronnoksessa tähän vastaa. SM korostaa erityisesti uusien matkaviestintä- ja viestintäteknisten palvelujen tuottamisvastuun ja integroituvan toimintaympäristön yhteistoiminnan määrittelyä selvästi palvelutuottajien kesken ERVEN tai sen tytäryhtiön vastuut tulee määrittellä asetuseronnoksessa esitettyä tarkemmin matkaviestintä- ja viestintäteknisten palveluiden tuottamisessa. Viranomaisradioverkon ja turvallisuusverkkotoiminnan yhteensulautumisesta tulee erityisesti huomioida näiden toimintaympäristöjen sekä niiden hallinnoinnin erilaisuus, jotta aiheutuvat integraatiohaasteet voidaan minimoida jo etukäteen.

SM esitti termien, määritelmien ja vaatimusten selkeyttämistä niin palvelu-, rajapinta- kuin kokonaistoimintakohtaisesti, jotta kaikki toimijat ymmärtävät omat vastuunsa ja voivat niiden täyttymisen selkeästi varmistaa.

SM totesi, että perustelumistion viestintäteknisten palvelujen kuvausten laadinnassa tulee huomioida, että palvelukuvaukset koskevat pääosin palveluoperaattorin teknistä toteutusta ja sen ylläpitoa. Palvelujen toiminnallinen hallinta tulee edelleenkin mahdollistaa niille aika- ja toimintakriittisille turvallisuusviranomaisille, joiden toiminnalliset tarpeet tätä edellyttävät. Viranomais-toimijoiden laaja käyttäjäkunta ja toiminnan erilaisuus edellyttävät monia eri ratkaisumalleja. Tehtävistä riippuen, käyttäjille on mahdollistettava räätälöidyt toteutusratkaisut keskeisiin sovelluksiin sekä toimialasidonnaisten mobiilipalvelujen käyttö, jotta vältetään tarpeettomalta usean eri laitteen käytöltä.

Useat pelastuslaitokset totesivat, että perustelumuiotiossa tulisi mainita, että palvelutuottaja on velvollinen varmistamaan asiakaskohtaisesti sekä turvallisuusverkon että viranomaisradioverkon palvelujen soveltuvuuden toiminnallisuuksien ja päätelaitteiden osalta jokaisen käyttövelvoitetun organisaation toimintaan. Palvelutuottajalla tulee olla velvoite tuottaa asiakkaille esimerkiksi toiminnassa edellytettävät tarkoituksen sopivat päätelaitteet lisälaitteineen asiakkaiden määritysten mukaisesti palveluna. Palvelutuottajan tulee myös huolehtia laitteiden varautumisen ja varaosien saatavuuden turvaamisesta yhteiskunnan eri olosuhteissa.

Itä-Uudenmaan pelastuslaitos totesi, että 3 §:n 3 momentin 1 kohdassa esitetään, että nykyisen viranomaisradioverkon päätelaitteet palvelut olisivat ERVEN tai sen tytäryhtiön tuottamia tieto- ja viestintäteknisiä palveluja. Huomioiden turvallisuusverkkolain 9 §:n mukainen palvelutuottajan yksinoikeus, pelastuslaitokselle jää epäselväksi, mahdollistaako luonnoksen mukainen menettely nykyisen käytännön jatkamisen, jossa viranomaisradioverkon päätelaitteita on voinut hankkia myös muilta laitetuottajilta kuin ERVEN tytäryhtiöltä (Virve Tuotteet ja Palvelut Oy). Nykyinen käytäntö tulee jo riittävän kilpailun turvaamiseksi varmistaa, sekä varmistua, että päätelaitteita voi hankkia markkinoilta laajasti myös siirryttäessä viranomaisten aikakriittisen laajakaistaisten matkaviestinnän palvelujen käyttöön.

Satakunnan pelastuslaitoksen mukaan palvelujen käyttäjillä tulee olla mahdollisuus hankkia toimintaansa tarvittavia laitteita, varaosia ja huoltopalveluita, vaikka tuotteiden toimituksissa olisikin viivästyksiä tiedossa palvelujen tuottajan suuntaan. Esimerkiksi tälläkin hetkellä Koronatilanteen vuoksi eri laite-, komponentti- ja varaosatoimittajien toimitukset viivästyvät eri toimittajien työn seisauksesta, joka osaltaan venyttää loppukäyttäjien laitteiden ja varaosien toimituksia. Tämän osalta palvelutuottajien tulisi varautua jollakin tasolla (3kk tai 6kk arvioitu puskurivarasto tai erittäin varma laitetuottaja).

Satakunnan pelastuslaitoksen mukaan palvelutuottajilla tulee olla keinot kasvattaa viranomaisradioverkon kapasiteettia paikallisesti (esim. suuronnettomuuden vaatima kapasiteetin kasvattaminen siirrettävillä väliaikaisilla tukiasemarakkaisuilla) ja mahdollisuus tuottaa myös väliaikainen verkon peittoalue sellaisille kriittisille alueille, joilla kuuluvuus madaltuu esimerkiksi tukiasematai muun vian sattuessa. Turvallisuusverkon käyttäjälle tulee myös mahdollistaa omatoiminen varautuminen, jolloin käyttäjä voisi halutessaan parantaa viranomaisradioverkon kapasiteettia tai luoda tilannepaikalle oman offline -lähi-verkon (esimerkiksi oma verkkopeitto suuren tapahtuman ajaksi).

## 2.2 Varautuminen (8 §)

Valtori piti ehdotettua täsmennystä ”palvelukohtaisten varautumista koskevien vaatimusten edellyttämässä laajuudessa” erinomaisena, sillä se mahdollistaa, että niin tietoturvan kuin varautumisen kannalta vähemmän kriittisten palvelujen järjestäminen on mahdollista käyttäen myös markkinoilta yleisesti saatavia ratkaisuja - ja näin keventää niiden hankintaan ja ohjaukseen liittyvää tekemistä ja kustannuksia.

SM:n mukaan varautumisen osalta on tärkeä tunnistaa ja huomioida palvelujen väliset riippuvuudet. Esimerkkinä sähköpostipalvelu poikkeusoloihin varautumisen osalta; mikäli tässä yhteydessä ei kokonaan tai osin huomioida esimerkiksi työasemapalveluja tai VPN-palvelua, ei varautuminen kokonaisuutena onnistu. Palvelujen välisiä riippuvuuksia korostetaan myös Valtioneuvoston 8.4.2020 antamassa päätöksessä valtion yhteisten tieto- ja viestintäteknisten palvelujen tuotannon ja käytön ensisijaisuus-, kiireellisyys- ja muussa tärkeysmäärittelyssä noudatettavista periaatteista ajalla 8.4.-15.5.2020.

Useat pelastuslaitokset totesivat, että asetuksella ei tule mahdollistaa, että palvelutuottaja pystyy alentamaan turvallisuusverkon palvelujen varautumisen tasoa keskeisissä viranomaisen turvallisuusverkon käyttövelvoitteen piirissä olevissa palveluissa.

Useat pelastuslaitokset totesivat myös, että perustelumuiotiossa tulee tarkentaa, että esitetyllä muutoksella palveluista voidaan tarjota asiakkaan toimintaan soveltuvia erilaisia tuotteita. Esimerkkinä asiakas voi valita tarkoituksen mukaisen tietoliikenneyhteyksratkaisun toimipisteeseen. Tietoliikenne ratkaisu voi olla perustason toteutus yksittäiseen toimipisteeseen, mutta sen tulee perustua turvallisuusverkon korkean varautumisen tietoliikenneinfrastruktuuriin. Uuden viranomaisradioverkon osalta on selkeästi tuotava esiin palvelukuvauksessa sen varautumisen taso ja soveltuvuus yhteiskunnan normaalioloissa ja poikkeusoloissa. Viranomaisradioverkon infra ja siihen liittyvät palvelut tulee olla tuotettu myös korkean varautumisen kriteerien mukaisesti. Tuotteistuksessa voidaan tarjota erilaisella varautumis- ja tietoturvasolla olevia tuotteita, joista asiakas valitsee toimintaansa soveltuvat. Palvelujen tuotannossa tulee huomioida, että turvallisuusverkon ja viranomaisradioverkon palvelujen tulee muodostaa ehjä palvelukokonaisuus. Viestinnän tulee olla mahdollista eri päätelaitteilla turvallisuusverkon ja viranomaisradioverkon välillä. Kustannustehokkuutta tulee hakea erityisesti keskittämällä viranomaisten palveluja yhteisiin tietoliikenne ratkaisuihin volyymin nostamiseksi ja eri viranomaisten osatointien välttämiseksi.

Oulu-Koillismaan pelastusliikelaitos esitti huolensa siitä, kuinka varmistetaan palvelujen jatkuvuuden turvaaminen normaalioloissa, niiden häiriötilanteissa sekä poikkeusoloissa. Asetuksen 8 §:n 1 momentti ja sitä koskeva perustelumuiotio nykyisessä muodossaan mahdollistaisi palveluntuottajan poikkeamisen varautumisvelvoitteista. Palvelukohtaisia varautumista koskevia vaatimuksia ei asetuksen 8 §:n 1 momentissa ja sitä koskevassa perustelumuiotiossa määritellä. Kriittisten ja käyttövelvoitettujen viranomaisradioverkon sekä viranomaisten aikakriittisen laajakaistaisen matkaviestinnän tieto- ja viestintäteknisten palvelujen varautumisen ei tulisi poiketa turvallisuusverkkolain hengestä.

Satakunnan pelastuslaitoksen mukaan asetuksessa tulee määritellä yhteisen turvallisuusverkon varautuminen sellaiselle tasolle, että turvallisuusverkon ja viranomaisradioverkon infrastruktuuri, tietoliikenne-, päätelaite- ja viestintäpalvelut sekä muut palveluja ja palvelutuottajia koskevat varautumisvelvoitteet toteutetaan korkean varautumisen kriteerien mukaisesti. Tämä tarkoittaa, että turvallisuus- ja viranomaisradioverkot toimivat häiriöttä mahdollisimman pitkään. Palvelujen ylläpitämiseksi palveluntuottajien tulee olla pitkälle omavaraisia (riittävät varalaitte ja varaosavarastot sekä luotettavat huoltopalvelut).

Satakunnan pelastuslaitoksen mukaan Virve 2.0. myötä viranomaisradioverkon viesti- ja datapalvelut siirtyvät Tetra-teknologiasta mobiilidataverkkoon, jonka tuottaa kaupallinen toimija ERVEn sopimuskumppanina. Toimijalla tulee olla riittävä varautumisen taso näiden palvelujen tuottamiseksi ja erityisen hyvin suunniteltu varautuminen kriittisten palvelujen ylläpitämiseksi. Esimerkiksi sähkökatkojen aikana palvelut tulisi olla käytettävissä vähintään 3 vrk (Keski-Euroopan mallilla), jonka aikana palveluntuottaja ehtii toimittamaan alueelle varavoimakoneen tai väliaikaisen siirrettävän tukiasemaratkaisun. Tällä velvoitteella saadaan myös palveluntuottaja päivittämään omien laitetilöiden ratkaisuja (sähkökytkennät) nykypäivän tasolle. Lisäksi viranomaisradioverkon kriittiset palvelut tulee olla määritelty sellaiselle tasolle, että kaupallinen toimija ei saa omatoimisesti priorisoida omia kaupallisia palveluja viranomaisten tasoa korkeammaksi (esim. korjausten priorisointi häiriötilanteen jälkeen).

## 2.3 Tietoturvallisuusvaatimukset (9 §)

Puolustusministeriön mukaan säännöstä tuli tarkentaa vaatimuksella siitä, että palvelutuottajan tulee palvelukohtaisesti ylläpitää luetteloa käyttäjäorganisaation tietoturvallisuusvaatimusten täyttymisestä. Lisäksi käyttäjäorganisaatiolle olisi ilmoitettava välittömästi asetuksen 10 §:n mukaisen arvioinnin tuloksista, arvioinnin puuttumisesta tai arvioinnissa tapahtuvista muutoksista. Esitetyllä muutoksella varmistettaisiin, että käyttäjäorganisaatiolla on käytössään ajantasainen tieto käyttämiensä ratkaisujen käyttöön ja tietoturvallisuuteen vaikuttavista tekijöistä. Käyttäjäorganisaatiolla on itsellään vastuu hyväksyä omien, eri turvallisuusluokkiin kuuluvien tietoaineistojen käsittely tietojärjestelmissä ja palveluissa. Hyväksyntään liittyy olennaisesti tieto järjestelmien ja palvelujen arvioinneista tai niiden puuttumisesta.

Edellä sanotun johdosta puolustusministeriö esitti asetuksen 9 §:ään lisättäväksi uuden 2 momentin seuraavasti:

*”Palveluntuottajan on ylläpidettävä palvelukohtaisesti eriteltyä luetteloa käyttäjäorganisaation tietoturvallisuusvaatimusten täyttymisestä sekä tietoturvallisuusvaatimusten arvioinnin tuloksista, puuttumisesta ja niissä tapahtuvista muutoksista. Palveluntuottajan on ilman aiheetonta viivytystä ilmoitettava tässä momentissa tarkoitetut tiedot kyseiselle käyttäjäorganisaatiolle.”*

Valtorin mukaan sen TORI- ja TUVE-liiketoimintojen yhteisen toiminnan osalta näiden tietoturvallisuus- ja tiedon luokitteluvaatimusten käsittely palvelukohtaisesti vähentänee tietojen yliluokittelua TUVE-toiminnassa ja helpottaa työskentelyä niin organisaation sisällä kuin mahdollisten alihankkijoidenkin kanssa.

SM piti esitettyä palvelujen skaalaamismallia hyvänä, ja erityisesti tämän seurauksena tehtävää palvelujen toiminnallisen käyttötarpeen ja käyttötilanteiden läpikäyntiä, jonka nähdään vain parantavan käyttöä vastaavien tietoturvallisuusvaatimusten määrittämistä. Lisäksi tulee ottaa huomioon erilaiset palvelujen käyttöympäristöt ja käytettävän yksittäisen tiedon lisäksi kokonaistarve.

SM:n mukaan palvelutuottajien välinen yhteistyö, tulisi asetuksessa varmistaa esimerkiksi kirjauksella:

*”Turvallisuusverkkolain 9 §:n 1 momentin ja 9 §:n 3 momentin palvelutuottajien välinen tehtäväjako sekä vastuut tulee toteuttaa siten että toiminta- ja aikakriittisille turvallisuustoimijoille osoitettavat kokonaispalvelut saadaan tuotettua turvallisuusviranomaisten tarpeiden edellyttämällä palvelutasolla.”*

SM:n mukaan asetusluonnoksesta ei selviä tarkoitetaanko kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004) tarkoitetuilla erityis-suojattaville tietoaineistoille asetetuilla tietoturvallisuusvaatimuksilla EU-tietoturvasääntöjä vai joidenkin valtioiden kanssa tehtyjä kahdenvälisiä turvallisuussopimuksia. Olisi myös hyvä mainita millä tasolla tietoturvallisuusvaatimukset täytetään (TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED).

Länsi-Uudenmaan pelastuslaitoksen mukaan turvallisuusluokitteluasetus (1101/2019) ei koske kunnallisia toimintoja. Perusteluissa todetaan, että 9 §:ssä ehdotetaan kuitenkin otettavaksi huomioon myös turvallisuusluokittelemattomien salassa pidettävien asiakirjojen käsittelyvaatimukset, tällainen on mm. julkisuuslaki. Mutta itse säädöstekstissä viitataan vain kansainväliseen tietoturvallisuusvelvoitteeseen, mutta ei julkisuuslakiin.

Satakunnan pelastuslaitos toteaa, että turvallisuusverkon tietoturvallisuus tulee olla prioriteetissa korkealla. Turvallisuusnäkökulman ohella tulee ottaa

huomioon palvelujen käytettävyys. Kriittisten palvelujen tulisi edelleen olla erittäin hyvin suojattuja ja sen myötä käytettävyydelle tulee olemaan haittavaikutuksia. Turvallisuusverkossa tulisi olla mahdollisuus käyttää kriittisiä palveluja siten, että ne ovat korkean tason suojauksen piirissä, jolloin nykyiset hitaat terminoidut palvelut saataisiin toimimaan nykyistä sujuvammin. Nykyisellään palvelujen käytettävyttä haittaavat useat eri kirjautumistavat ja palvelutuottajien suuntaan rakennetut keinotekoiset terminoidut yhteydet.

## 2.4 Turvallisuusverkon palvelujen käyttö (11 §)

SM piti tärkeänä muutosta, jonka mukaan palvelutuottajan ei tarvitse hankkia käyttäjän tietojärjestelmän tai tieto- ja viestintäteknisen palvelun liittämiseksi valtiovarainministeriön hyväksyntää, mikäli palvelutuottaja pystyy varmistamaan liittämiseksi asetettujen vaatimusten täyttymisestä. Tämä edesauttaa, etteivät operatiivisen toiminnan ja lainsäädännön edellyttämien muutosten aikataulut eivätkä vaatimustenmukaisten tietojärjestelmien käyttöönotot viivästy hallinnollisten käsittelyiden seurauksena tarpeettomasti. SM kuitenkin korosti liittämisen vaatimusten määrittelyn huomattavaa selkeyttämistä. Lisäksi tulee huomioida, että turvallisuusverkkolain mukaisesti valtiovarainministeriöllä säilyy tieto- ja viestintäteknisen varautumisen ja turvallisuuden valvontavastuu.

SM:n mukaan tulee määritellä yksiselitteisen selkeästi mitä toimialasidonnaisella tietojärjestelmällä tai tieto- ja viestintäteknisellä palvelulla tarkoitetaan tässä yhteydessä, ja mitkä ovat edellä mainittujen osalta rajapinnat TUVE-verkkoon ja/tai siinä tarjottaviin palveluihin nähden. Toisin sanoen, sisällytetäänkö johonkin viranomaisen toimialasidonnaisen järjestelmän tai palvelun kuvaukseen myös TUVE-verkko tai TUVE-palveluja. Näin ei pitäisi olla ainaakaan tiedonsiirron osalta. Sen osalta rajapinta voisi olla OSI mallin mukaisten 3. ja 4. kerrosten välillä, jolloin toimialasidonnaisten järjestelmien ulkopuolelle jäisivät kerrokset 1 - 3. TUVE-palvelujen osalta vastuurajat tulisi määritellä yksiselitteisesti.

SM:n mukaan myös ”määrätyt tietoturvallisuusvaatimukset” tulisi määritellä selkeästi. Mikäli kaikille yhteisiä tietoturvallisuusvaatimuksia ollaan antamassa, tulisi se antaa viimeistään asetuksen muutoksen yhteydessä. Tietoturvallisuusvaatimusten tulisi olla yksiselitteiset, mielellään standardeihin tai muihin yleisesti tunnettuihin ja hyväksytyihin perustuvia sekä ennen kaikkea myös Traficomien hyväksymät. Lisäksi edellä mainitut vaatimukset tulee voida luovuttaa järjestelmää tai palvelua kehittäväälle ulkopuoliselle taholle, jotta vaatimusten täytyminen voidaan selkeästi todentaa ennalta tiedossa olevin, yhtenäisin mittarein. Tietoturvallisuusvaatimusten yksiselitteisyys on edellytys myös momentin viimeisessä lauseessa käyttäjälle säädetyin selvitysvelvollisuuden täyttämiseksi.

Helsingin kaupungin pelastuslaitoksen mukaan palvelutuottajan on ilmoitettava ennakkoon soveltamansa tietoturvallisuusvaatimukset kussakin käyttäjätapauksessa. Lisäksi 11 §:n loppuun tulisi lisätä palvelutuottajalle velvollisuus viipymättä ja luotettavasti tiedottaa käyttäjälle palvelujen suorituskykyä tai tietoturvallisuutta vaarantavista tilanteista, jotka voivat vaikuttaa palvelujen käyttöön. Viranomaisten määrittelemät kriittiset palvelut on asetettava etusijalle rajoitustilanteissa. Palvelutuottajan on mitattava ja tuotettava säännöllisesti tietoa palvelujen laadusta palvelujen käyttäjille.

Itä-Uudenmaan pelastuslaitoksen mielestä 11 §:n 2 momentissa esitetty vaatimus käyttäjälle selvittää palvelutuottajalle tietoturvallisuusvaatimusten täyttymisen on turha ja myös ristiriidassa turvallisuusverkkolain 2 ja 3 §:n käyttövelvoitteen kanssa. Käyttövelvoitteen piirissä olevat tahot vastaavat isäntäorgani-



saationsa (tiedonhallintalain mukainen tiedonhallintayksikkö) kautta lainmukaisen tietoturvallisuuden ylläpitämisestä, eikä sitä tule saattaa palvelutuottajan arvioitavaksi.

Itä-Uudenmaan pelastuslaitoksen mukaan 11 §:n perusteluihin tulisi lisätä kuvaus menettelyistä toimialasidonnaisen palvelun hyväksymisestä, niin turvallisuusverkkoon, kuin erityisesti viranomaisradioverkkoon. Pelastuslaitoksilla on käytössään useita toimialasidonnaisia viranomaisradioverkossa toimivia palveluja, ja näiden palvelujen käyttö tulee turvata myös jatkossa.

Usean pelastuslaitoksen mukaan turvallisuusverkossa tulisi olla mahdollisuus palvelujen skaalautuvuuteen, jolloin kolmannen osapuolen käyttäjiä saadaan lisättyä sujuvasti esimerkiksi viranomaisradioverkon palveluihin. Tällaisissa tapauksissa kolmannen osapuolen tietoturvan tasoa ei välttämättä voida varmentaa luotettavasti. Tämän tyyppistä käyttöä voisi olla viranomaisissa esimerkiksi asiantuntijoiden, laitteiden ja koneiden käyttäjien, etsintäpartioiden henkilöiden lisääminen viestipalveluihin. Näissä tapauksissa tieto voisi olla lähtökohtaisesti julkista ja palvelujen varmentamista ei välttämättä tarvitsisi tehdä. Henkilöt tai henkilöryhmät voisivat käyttää viranomaisradioverkon palveluja sujuvasti esimerkiksi omaan puhelimeen ladattavalla applikaatiolla, käyttäisivät omia matkapuhelinyhteyksiä ja toimisivat turvallisuusverkon julkisella tai sitten salassa pidettävällä alueella. Mallina voitaisiin pitää ad-hoc. Viranomaisten viestintätekniisten palvelujen kannalta on tärkeä tunnistaa, että itse viestintätekniistä palvelua tulee voida käyttää tarvittaessa muillakin kuin viranomaisverkon liittymillä ja päätelaitteilla. Viranomaisen tulee pystyä esimerkiksi viestimään viranomaisen välineillä myös julkisessa viestintäverkossa oleviin päätelaitteisiin (asiantuntijat, kolmannet osapuolet, omat henkilöstöt, jne.). Varautumisen parantamiseksi tulee arvioida myös viranomaisradioverkon ja julkisen verkon yhtäaikaista käyttöä samassa päätelaitteissa. Turvallisuusverkon käyttäjille tulee mahdollistaa omat testausympäristöt, jolla he voivat koestaa niin TUVE, kuin Virve –palvelujen laitteita ja sovelluksia sekä niiden käytettävyyttä.

Usean pelastuslaitoksen mukaan turvallisuusverkon ja viranomaisradioverkon palvelujen tuotannon tulisi muodostaa ehjä palvelukokonaisuus. Viestinnässä tulee olla mahdollisuus eri päätelaitteiden käyttämiseen niin turvallisuusverkossa, kuin viranomaisverkossa ja niiden välillä. Esimerkiksi Virve –päivystäjän työasemaa voisi käyttää TUVE -verkon ylitse, jolloin ei tarvitse hankkia erikseen omaa, vain Virve –käyttöön pyhitettyä työasemaa. Kustannustehokkuutta tulee hakea erityisesti keskittämällä viranomaisten palveluja yhteisiin tietoliikennetarkaisuihin volyymien nostamiseksi ja eri viranomaisten osaoptimointien välttämiseksi.

## 2.5 Muut asiat

Puolustusministeriön mukaan turvallisuusverkon palvelutuotannon kustannusrakenteissa ei saisi tapahtua kustannusten nousuun johtavia muutoksia.

Valtori totesi, että on tärkeää, että lakeja ja asetuksia muutetaan vastaamaan paremmin vallitsevaa tilannetta. Korona-pandemia on opettanut julkista sektoria erittäin paljon seuraavissa asioissa:

- oikea-aikaisen reagoinnin tärkeys
- eri toimijoiden yhteistyön ja yhteisen varautumisen tärkeys, ei ole mielekästä, että esim. kaikki toimijat rakentavat omia varajärjestelmiään, vaan että eri toimijoiden järjestelmät voivat toimia toistensa varajärjestelminä (myös esim. jotkin TORI-palvelut olisivat voineet toimia TUVE varajärjestelminä, jos ne olisi alun perin suunniteltu tämän huomioiden)
- kansalaisten ja yhteiskunnan turvallisuus ja toimivuus poikkeusoloissa on aiempaa laajemmin tieto- ja viestintätekniisten toimivuuden varassa

Valtorin mukaan olisi tärkeää, että esim. syksyllä 2020 perustetaan VM:n ja julkisen sektorin keskeisten ICT-toimijoiden työryhmä, joka kokoaa yhteen kaikki "opit", jotka tästä on saatu ja tekee ehdotuksen VM:lle ja/tai muille ministeriöille siitä, kuinka toimintaa voidaan niin lainsäädännön kuin muinkin keinoin kehittää. Valtori on halukas osallistumaan sanotun työryhmän toimintaan.

SM:n mukaan tiedonhallintalaissa tiedonhallintayksikölle asetetun riskiarviointivelvollisuuden tulisi näkyä asetuksessa selkeästi. Perustelumuiustiossa riskiarvio on otettu esiin osana poikkeamapäätösten hyväksymis- ja käyttöönottomennettelyjä. Riskiarvion tulisi olla kiinteä osa palvelujen suunnittelu-, kehittämis- ja käyttöönottoaiheita.

Kilpailu- ja kuluttajaviraston näkemyksen mukaan asetusluonnokseen ei lähtökohtaisesti sisälly kilpailuneutraliteettia vaarantavia piirteitä. Se kiinnitti kuitenkin huomiota siihen, että turvallisuusverkkolaissa ja -asetuksessa tarkoitettujen palvelutuottajat voivat mahdollisesti toimia joillakin toisilla markkinoilla kilpailutilanteessa yksityisten yritysten kanssa. Esimerkiksi ERVE-konserniin kuuluva Johtotieto Oy toimii kilpailuilla markkinoilla muun muassa infrastruktuuriverkkojen sijaintitietopalvelujen tuottajana. Kilpailuneutraliteetti voi vaarantua, mikäli palvelutuottajat voivat hyödyntää alihintaan esimerkiksi turvallisuusverkon tai viranomaisradioverkon ylläpidossa tarvittavaa osaamista tai muita resursseja kilpailuilla markkinoilla tapahtuvassa toiminnassa. Kilpailulain (948/2011) 30 d § edellyttää lähtökohtaisesti, että kilpailutilanteessa markkinoilla harjoitetusta taloudellisesta toiminnasta on pidettävä erillistä kirjanpitoa. Kilpailuilla markkinoilla syntyvät kustannukset tulee aina kohdentaa aiheuttamisperiaatteen mukaisesti.

UM ei niinkään lausunnossaan ottanut kantaa itse asetustekstiin, mutta esitti yleisempiä näkemyksiä TUVE-toimintamallista ja sen kehittämistarpeesta.

ERVE totesi, että turvallisuusverkkolakia tulee muuttaa siten että TUVE-toiminnassa asiakirjat luokitellaan asiakirjojen turvallisuusluokittelusta valtionhallinnossa annetun asetuksen mukaan.

### 3 Lausuntopalautteen vaikutus

Kaikki saatu lausuntopalaute on valtiovarainministeriössä eritelty ja koottu jatkovalmistelua varten. Tässä lausuntoyhteenvedossa ei ole käsitelty lausuntojen aiheuttamia muutoksia asetusehdotukseen. Tehdyt muutokset esitettävään asetukseen kirjataan jatkovalmistelun jälkeen keskeisiltä osin asetuksen perustelumuiustioon.

Jakelu Lausuntokooste julkaistaan valtioneuvoston hanketietosivulla