Tietoliikenteen ja tietotekniikan keskusliitto, FiCom ry

Lausunto

15.02.2024

Asia: VN /5137/2022

Työryhmän lausuntopyyntö valmiuslain varautumisvelvollisuutta koskevasta muistiosta sekä valmiuslain yleisistä kehittämistarpeista

Lausunnonantajan lausunto

Huomionne valmiuslain varautumisvelvollisuutta koskevasta muistiosta

FiComin keskeiset viestit:

- Muistio on kattava, selkeä ja kannatettava.
- Yksityisen sektorin jättäminen valmiuslain yleisen varautumissääntelyn soveltamisalan ulkopuolelle on kannatettavaa ja tarkoituksenmukaista.
- Yhteiskunnan toimivuuden kannalta kriittiset järjestelmät ja palvelut ovat yhä useammin lähes kokonaan yksityisen sektorin tuottamia. Viranomaisten on siksi tehtävä entistä enemmän yhteistyötä yritysten kanssa.
- Keskinäisriippuvaisessa ja digitalisoituneessa yhteiskunnassa tulisi panostaa etenkin kansainvälisten yhteyksien ja logistiikkaketjujen toimivuuteen.
- Valmiuslain kokonaisuudistus ja erityisesti lain sähköisiä tieto- ja viestintäjärjestelmiä koskevan 9 luvun päivittäminen on tärkeää, koska teknologinen kehitys ja toimintatapojen muutos on viime vuosien aikana ollut huomattavaa. Samalla tulee päivittää sähköisen viestinnän palvelulain varautumista koskeva 35 luku sekä lain määritelmät ja soveltamisala.
- Yksityiskohtaisten säännösten ja keinojen säätämisen sijasta varautumissääntelyn tulee olla tavoitepohjaista.
- Varautumiskustannuksia aiheutuu normaalioloissa, poikkeusoloissa ja normaaliolojen häiriötilanteissa, mutta myös niistä palauduttaessa.
- Jatkovalmistelussa tulisi arvioida erityisesti kriittisten toimialojen työvelvoitetta poikkeusolojen ja normaaliaikojen häiriötilanteissa. Lisäksi jatkovalmistelussa tulisi paremmin huomioida se, että poikkeusolot tai normaaliolojen häiriötilanteet voivat olla alueellisia ja/tai paikallisia. Tästä voidaan tarvittaessa säätää myös toimialakohtaisessa erityislainsäädännössä.

- Valmiuslain poikkeusvaltuuksien käyttöönottokynnyksen tulee jatkossakin olla korkea. Siksi on tärkeää, että normaaliaikojen valtuuksiin perustuva lainsäädäntö mahdollistaa häiriö- ja kriisitilanteissa toimimisen mahdollisimman pitkään

Huomionne valmiuslain varautumisvelvollisuutta koskevasta muistiosta

FiCom pitää muistiota kattavana, selkeänä ja kannatettava. On tarpeellista, että julkisen sektorin varautumista arvioidaan kokonaisuutena, koska se on tärkeä osa kokonaisturvallisuutta. Samalla kuitenkin tunnistetaan ja tunnustetaan yksityisen sektorin kasvanut rooli ja merkitys. Muistion ehdotus siitä, että julkishallinnon valmiuslain mukaisen yleisen varautumisvelvollisuuden tulisi koskea sekä poikkeusoloihin varautumista että jatkossa myös normaaliolojen häiriötilanteita, on kannatettava ja tarpeellinen.

FiCom yhtyy muistion näkemykseen siitä, että yksityisen sektorin, myös toimiluvanvaraisten toimijoiden, jättäminen valmiuslain yleisen varautumissääntelyn soveltamisalan ulkopuolelle on kannatettavaa. Yksityisen sektorin kriittisten toimijoiden varautumista tulee jatkossakin vahvistaa ensisijaisesti toimialakohtaisen erityislainsäädännön kautta. Kunkin sektorin erityispiirteet tulee ottaa huomioon, kuten on tehty teleyritysten kohdalla sähköisen viestinnän palvelulaissa (SVPL). On kuitenkin vältettävä päällekkäistä hallinnollista taakkaa ja kustannuksia aiheuttavia velvoitteita. Asia tulee huomioida valmiuslain jatkovalmistelussa, mutta ennen kaikkea tulevissa verkko- ja tietoturvadirektiivissä (NIS2), kriittisen infrastruktuurin direktiivissä (CER) sekä kyberkestävyyssäädöksessä (CRA).

Muistiossa kuvataan viranomaisen tarve varmistua sopimusjärjestelyin varautumisen toteutumisesta kriittisten tehtävien jatkuvuuden varmistamiseksi. Esimerkkinä mainitaan tieto- ja viestintätekniset ja kriittiseen toimintaan vaikuttavat hankinnat (s. 19 ja 26). Sopimusjärjestelytilanteissa tulee varmistua siitä, että ei luoda sektorikohtaisen varautumissääntelyn kanssa päällekkäisiä tai ristiriitaisia sopimusvelvoitteita. Toisin sanoen erillisille sopimusjärjestelyille ei ole tarvetta silloin, kun toimittaja on jo lakisääteisen varautumisvelvoitteen piirissä.

Muistiossa on tunnistettu oikeat kehitystarpeet ja tuotu hyvin esille yhteiskunnassa tapahtuneet muutokset, mm. Ukrainan sota, digitalisoituminen sekä keskinäisriippuvuudet. Olemme yhä enemmän riippuvaisia toistemme palveluista (esimerkiksi energiayhtiöt teleyritysten palveluista ja päinvastoin). On tärkeää, että muutokset tunnistetaan.

Lisäksi on tärkeää huomata, että toimialoilla, esimerkiksi telealalla, tapahtuu merkittäviä muutoksia ja jatkuvaa teknologista kehitystä hyvin nopeaan tahtiin. Muutos korostaa, että sektorikohtaisen varautumissääntelyn tulee olla aikaa kestävää ja tavoitepohjaista, ei yksityiskohtaista ja keinoja sisältävää.

Yksityisen sektorin ja keskinäisriippuvuuden tunnistaminen ja tunnustaminen

Muistiossa on hyvin tuotu esille ja ylipäänsä tunnistettu se, että yhteiskunnan toimivuuden kannalta kriittiset järjestelmät ja palvelut ovat yhä useammin lähes kokonaan yksityisen sektorin tuottamia. Yhteiskunnan digitalisoituessa yritysten asema etenkin tieto- ja viestintäteknisten palveluiden tuottamisessa ja kybertoimintaympäristön turvaamisessa on muodostunut varsin keskeiseksi. Monet yhteiskunnan toiminnan kannalta elintärkeät palvelut, kuten maksuliikenteen välitys, sähköverkot ja vedenjakelu, ovat riippuvaisia viestintäpalveluiden ja -verkkojen toiminnasta.

Muistiossa tunnistettiin hyvin, että kansainväliset yhteydet ovat monelle toimialalle elintärkeitä. Esimerkiksi yrityselämän ja osin julkisen hallinnon tietotekniset palvelut ovat riippuvaisia tietoliikenneyhteyksistä ulkomaisiin palvelinkeskuksiin. Niiden toimivuushäiriöt muodostavat merkittävän uhan yhteiskunnan toiminnalle, koska häiriötilanteissa ongelmia ei välttämättä voida ratkaista kansallisesti. Eri sähköisten järjestelmien ja palveluiden keskinäisriippuvuuksien vuoksi vikojen ja häiriöiden ketjuuntuminen ja kertautuminen ovat merkittävä uhka (s. 20), unohtamatta toimitus- ja logistiikkaketjuja. Tästä syystä kansainvälisten yhteyksien toimivuutta tulisi tarkastella kokonaisvaltaisesti myös kansallisella tasolla. Tavoitteena tulisi olla se, että kansainväliset yhteydet toimivat mahdollisimman hyvin myös kriisitilanteissa. Keskinäisriippuvaisessa ja digitalisoituneessa yhteiskunnassa tulisi panostaa myös kansainvälisten yhteyksien toimivuuteen. Varautumisen kannalta on kriittistä, että meillä on mahdollisuus tukeutua Suomen ulkopuolella sijaitseviin resursseihin, joten on tärkeää varmistaa, että tälle ei aseteta lainsäädännöstä johtuvia tarpeettomia estettä.

Teleyritykset huolehtivat palveluiden kansallisesta ja kansainvälisestä toimivuudesta omalta osaltaan. Tällöin on tärkeää, että heidät pidetään mukana valmistelussa, myös silloin kuin ei käsitellä juuri heitä koskevaa sääntelyä. Keskinäisriippuvuuden takia esimerkiksi ICT-alaa kiinnostaa energiatoimialaa koskeva sääntely.

Kriisijohtaminen ja yhteistyö

Muistiossa mainitussa selvityksessä nostettiin esille tarve arvioida kriisijohtamisen rakenteiden kehittäminen ja normaaliolojen häiriötilanteiden johtamismallien hyödyntäminen myös kriisiaikoina (s. 21). Myös huomiot yhteistyöstä eri toimijoiden, toimialojen ja useiden hallinnonalojen ja yksityisen sektorin välillä, poikkihallinnollinen yhteensovittaminen sekä havainto siitä, että nykyaikaiset turvallisuusuhat eivät noudata hallinnonalarajoja, olivat relevantteja. (s. 25) Lisäksi johtamisjärjestelmän toimivuus ja koordinointi sekä toiminnan harjoitteleminen ennalta ovat keskeisessä asemassa.

Kannatettavaa on työryhmän ehdotus siitä, että ministeriöiden hallinnonalojen ohjausta koskevaa sääntelyä tulisi täydentää säätämällä ministeriöille velvollisuus huolehtia toimialallaan varautumisen ohjauksesta, yhteensovittamisesta ja valvonnasta tarvittavissa määrin yhteistyössä/yhteistoiminnassa muiden ministeriöiden kanssa.

Normaaliolojen toimintamallien tulee olla mahdollisimman pitkälle käytössä myös valmiuslain mukaisissa poikkeusoloissa. Johtamisjärjestelmän ja vastuiden selkeys myös poikkeustilanteissa sekä erilaisten skenaarioiden harjoitteleminen on tärkeää, jotta toimivaltuuksien käyttöä ja niihin liittyviä haasteita ja vaikutuksia voidaan myös käytännössä arvioida. Johtaminen ja organisointi on tehtävä yhdessä yksityisen sektorin kanssa, jotta mallit toimivat aidosti myös käytännössä. Samoin yhteistyötä ja tiedonkulkua tulisi kehittää kansallisesti erityisesti kriittisten yksityisen sektorin toimijoiden kanssa.

Miten arvioisitte voimassa olevan valmiuslain kokonaisuutta ja toimivuutta? Mitä valmiuslaissa tulisi erityisesti kehittää?

Valmiuslakia tulee tarkastella uudella tavalla – siinä on huomioitava teknologisen kehityksen tuoma toimintatapojen muutos ja muu sääntely.

Valmiuslain kokonaisuudistus ja päivittäminen on tärkeää. Tämä koskee erityisesti valmiuslain 9 luvun sähköisiä tieto- ja viestintäjärjestelmiä, koska niiden teknologinen kehitys ja toimintatapojen muutos on viime vuosina ollut huomattavaa. Lain tavoite, sen määritelmät, soveltamisala ja toimivaltuudet eivät ole enää yksiselitteisiä eivätkä ajanmukaisia.

Valmiuslain kokonaisuudistuksen yhteydessä tulisi arvioida voimassa olevan sähköisen viestinnän palvelulain (SVPL) varautumissääntelyn ajantasaisuus, mikä on kiinteästi kytköksissä myös valmiuslain sääntelyyn. SVPL:n varautumissääntely, joka koskee esimerkiksi viestintäverkon kriittisen järjestelmän palauttamista Suomeen (SVPL 283 §), on laadittu ennen ICT-toimialan nopeaa ja voimakasta kehitystä sekä ennen Ukrainan sotaa, josta saatavat opit tulee hyödyntää myös valmiuslain uudistuksessa.

Ukrainan sodassa on muun muassa havaittu, että rajat ylittävä yhteistyö on parantanut Ukrainan viestintäverkkojen ja -palvelujen resilienssiä. Yksityiskohtaisten säännösten ja keinojen säätämisen sijasta varautumissääntelyn tulee olla tavoitepohjaista: sen tulee kannustaa entistä turvallisempien palvelujen luomiseen ja mahdollistaa viestintäverkkojen ja -palvelujen resilienssin vahvistaminen myös edistämällä rajat ylittävää yhteistyötä EU- ja Nato-maiden välillä. Esimerkiksi tietojen hajauttaminen pilvipalveluihin parantaa verkkojen ja palvelujen turvallisuutta. Pilvestä tiedot ovat saatavilla niin poikkeusolojen aikana kuin myös tilanteessa, jossa yhteiskuntaa aletaan poikkeusolojen jälkeen palauttaa ja kehittää takaisin normaaliaikojen tilanteeseen. Kansallisesti kriittinen data ei nykyisin ole parhaiten turvattu vain valtakunnan rajojen sisäpuolella.

Julkisen ja yksityisen sektorin yhteistyötä voi edelleen tiivistää. Tämä tulisi huomioida myös valmiuslain mahdollisia toimivaltuuksia käytettäessä. Yksityinen sektori tulisi ottaa mukaan esimerkiksi silloin, kun sitä koskevia toimivaltuuksia aiotaan ottaa käyttöön. Nykyinen valmiuslaki ei

tätä tunnista. Julkisen ja yksityisen sektorin yhteistyö on Suomen vahvuus ja on tärkeää pitää siitä kiinni.

Onko muita näkökulmia, joita edustamanne taho erityisesti toivoisi otettavan huomioon valmiuslain uudistamista koskevassa työssä?

FiCom viittaa lausuntoonsa valmiuslain toimivaltuussäännösten uudistamisesta, mutta toteaa tiivistetysti seuraavaa.

Monet voimassa olevat valmiuslain vaatimukset voivat edellyttää investointeja ja ylläpitokustannuksia normaalioloissakin. Varautumiskustannusten lisäksi myös poikkeusoloista ja normaaliolojen häiriötilanteista aiheutuva toipuminen aiheuttaa kustannuksia. Valmiuslaissa ei ole säännöksiä siitä, mitä tapahtuu ja tehdään, kun poikkeusolot ja normaaliolojen häiriötilanne ovat päättyneet. Varautumista, vastuita ja erityisesti korvauksia koskevia säännöksiä valmiuslain 128 § ja SVPL 298 § tulisi arvioida lain jatkovalmistelussa.

Valmistelun jatkotyössä olisi syytä arvioida kriittisten toimialojen työvelvoitetta poikkeusolojen ja normaaliaikojen häiriötilanteissa . Tämä koskee erityisesti edellä kuvatun mukaisesti viestintäpalveluita ja -verkkoja ja niiden keskeistä roolia muiden kriittisten toimintojen ylläpitämisessä.

Jatkovalmistelussa tulisi paremmin ottaa huomioon se, että poikkeusolot tai normaaliolojen häiriötilanteet voivat olla alueellisia ja/tai paikallisia (muistion s. 22, 23 ja 29).

Valmiuslain poikkeusvaltuuksien käyttöönottokynnyksen tulee jatkossakin olla korkea. Siksi on tärkeää, että normaaliaikojen valtuuksiin perustuva lainsäädäntö mahdollistaa häiriö- ja kriisitilanteissa toimimisen mahdollisimman pitkään. Samanaikaisesti tulee kuitenkin tiedostaa, etteivät valmiuslain poikkeusoloja koskeva tiukat velvollisuudet ja vaatimukset de facto muutu normaaliolojen velvollisuuksiksi sähköisen viestinnän palvelulaissa .

Varautumista ja normaaliolojen häiriötilanteita koskeva erityissääntely

SVPL:ssä on oma varautumista koskeva lukunsa (35), jonka mukaan teleyrityksen on muun muassa huolehdittava siitä, että sen toiminta jatkuu mahdollisimman häiriöttömästi myös normaaliolojen häiriötilanteissa sekä valmiuslaissa tarkoitetuissa poikkeusoloissa. Tämä luku kaipaa päivitystä, jotta se olisi ajanmukainen, selkeä ja tasapainoinen uudistettavan valmiuslain kanssa. Uudistamista kaipaavat myös SVPL:n määritelmät (mikä on teleyritys) ja soveltamisala (pilvipalvelu), joiden osalta FiCom viittaa mainittuun aiempaan lausuntoonsa. Lait ovat viittauksiensa vuoksi sidoksissa toisiinsa, joten SVPL: päivittämättä jättäminen aiheuttaa merkittäviä soveltamisongelmia, jotka tulee ratkaista etukäteen.

Säännösten perusteella teleyrityksen on tehtävä varautumissuunnitelma valmiuslain 9 luvun mukaisia toimivaltuuksia käytettäessä, tai Suomeen on voitava palauttaa viipymättä kriittinen viestintäverkon järjestelmä sekä sen ohjaus, ylläpito ja hallinta käytettäessä valmiuslain 60 §:n 1 momentin 8 kohdan mukaista toimivaltuutta. Esimerkiksi tämä viimeinen palauttamista koskeva sääntely edellyttää päivittämistä. Teleyrityksen on siis jo omassa SVPL:n mukaisessa varautumissuunnittelussaan arvioitava ja otettava huomioon, miten se pystyy huolehtimaan toimintansa jatkuvuudesta myös poikkeusoloissa.

SVPL sisältää runsaasti viestintäverkkojen ja -palvelujen suunnittelua, varautumista ja laatuvaatimuksia koskevia säännöksiä (243 ja 244 §) ja määräyksiä, jotka teleyrityksen on otettava huomioon suunniteltaessa, rakennettaessa ja ylläpidettäessä yleisiä viestintäverkkoja ja -palveluita. Lain 243 § 14 kohdan mukaan viestintäverkkojen ja -palveluiden tulee toimia mahdollisimman luotettavasti myös valmiuslaissa (1552/2011) tarkoitetuissa poikkeusoloissa ja normaaliolojen häiriötilanteissa.

Kansallisten säädösten lisäksi EU:sta on tullut ja tulossa merkittävässä määrin uutta kyberturvallisuuteen ja resilienssiin keskittyvää sääntelyä, kuten verkko- ja tietoturvadirektiivi (NIS2) ja kriittisen infrastruktuurin direktiivi (CER) sekä tuleva kyberkestävyyssäädös (CRA). Näillä kaikilla on vaikutusta varautumiseen ja häiriötilanteiden hallintaan myös valmiuslain mukaisissa poikkeusoloissa, joten niistä seuraavat varautumis- tms. velvoitteet tulee huomioida valmiuslakia uudistettaessa ja välttää päällekkäisyyksiä sekä hallinnollista taakkaa. Tältä osin muistion huomiot ovat kannatettavia (s. 24 ja 25).

Lopuksi FiCom toteaa, että koronapandemian aikana viestintäverkot toimivat laadukkaasti, mikä osoittaa sen, että käytännön tasolla myös toimintamallit ovat hyviä. Edellä kuvatun mukaisesti, paitsi valmiuslaki mutta myös SVPL kaipaa päivittämistä.

Lahtinen Marko
Tietoliikenteen ja tietotekniikan keskusliitto, FiCom ry