LAUSUNTO HALLINTOVALIOKUNNALLE

Asia:

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

Hallintovaliokunta on pyytänyt minulta asiantuntijalausuntoa hallituksen esityksestä 63/2022 vp. Käsittelen lausunnossani eräitä hallituksen esityksen lähtökohtia ja käsitteitä suhteessa julkisen hallinnon tieto- ja viestintäteknisten palvelujen ohjaamiseen, järjestämiseen ja tuottamiseen.

Esitän valiokunnalle lausuntonani kunnioittavasti seuraavaa:

1. Yleistä – julkisen hallinnon tieto- ja viestintäteknisten palvelujen merkitys yhteiskunnan toiminnalle

Hallituksen esityksen 1. lakiehdotuksen tarkoituksena on vähäisessä määrin ajantasaistaa voimassa olevaa valmiuslakia siten, että siinä huomioitaisiin kattavammin hybridiuhat, jotka voisivat johtaa yhteiskunnan tilanteeseen, jossa tarvitaan poikkeusoloja varten säädettyä sääntelyä. Ehdotus mahdollistaisi eräiden toimivaltuuksien käytön poikkeuksellisissa ja laajoissa hybridiuhkatilanteissa. Ehdotus sisältää jonkin verran viranomaisille uusia toimivaltuuksia, mutta poikkeusolojen määritelmä itsessään laajentaa voimassa olevan valmiuslain viranomaisten toimivaltuuksia koskevien säännösten käyttöalaa. Tässä suhteessa ehdotetulla sääntelyllä on ainakin teoriassa merkittäviäkin vaikutuksia viranomaisten toimivaltuuksiin hybridiuhkiin liittyvissä tilanteissa.

Nyt ehdotettava sääntely voisi tulla sovellettavaksi vain hyvin poikkeuksellisissa olosuhteissa. Perustuslain 23 §:n mukaan perusoikeuksista voidaan säätää lailla tai laissa erityisestä syystä säädetyn ja soveltamisalaltaan täsmällisesti rajatun valtuuden nojalla annettavalla valtioneuvoston asetuksella sellaisia tilapäisiä poikkeuksia, jotka ovat välttämättömiä Suomeen kohdistuvan aseellisen hyökkäyksen samoin kuin muiden kansakuntaa vakavasti uhkaavien, laissa säädettyjen poikkeusolojen aikana ja jotka ovat Suomen kansainvälisten ihmisoikeusvelvoitteiden mukaisia. Lailla on kuitenkin säädettävä tilapäisten poikkeusten perusteet. *Perustuslain 23 §:ssä säädetystä johtuen valmiuslain poikkeusoloja koskevan määritelmän tilanteet eivät voi tulla sovellettavaksi erilaisissa yhteiskunnan perusinfrastruktuuriin kohdistuvissa tahattomissa tai tahallisissa häiriötilanteissa, jotka ovat ennakoitavissa ja joihin voidaan reagoida viranomaisten normaalioloja koskevien toimivaltuuksien puitteissa.*

Suomen julkinen hallinto toimii monin osin tietojärjestelmien ja tietoverkkojen varassa. Viimeisen parin kymmenen vuoden aikana tietojärjestelmäpalveluja on keskitetty viranomaisten yhteisiksi palveluiksi. *Tällainen keskittäminen itsessään voi muodostaa merkittäviä riskejä viranomaisten toiminnalle erityisesti kyberuhkatilanteissa, koska yksittäiseenkin järjestelmään kohdistuvalla kyberiskulla voi olla huomattavan laajat ja lamaannuttavat vaikutukset julkisen hallinnon viranomaistoimintaan*. Toisaalta keskittämisen pitäisi parantaa mahdollisuuksia varautua erilaisiin häiriötilanteisiin.

Valtionhallinnossa perustietotekniikkapalveluja ja osin tietojärjestelmäpalveluja tuotetaan valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä annetun lain (1226/2013, tietotekniikkapalvelulaki) ja sen nojalla annetun sääntelyn perusteella. Tietotekniikkapalvelulain 15 §:ssä on säädetty palvelujen tuottajien velvollisuuksista varautua normaaliolojen häiriötilanteisiin sekä poikkeusoloihin. Mainitun lainkohdan mukaan ”Ellei muussa laissa toisin säädetä, normaalioloissa ja niiden häiriötilanteissa noudatetaan tässä laissa tarkoitettujen palvelujen tuotannon ja käytön ensisijaisuus-, kiireellisyys- ja muussa tärkeysmäärittelyssä valtiovarainministeriön ennalta määrittelemiä periaatteita.

Valtiovarainministeriön on ennen periaatteiden vahvistamista kuultava asianomaisia palvelujen tuottajia, asiakkaita ja ministeriöitä. Valtioneuvosto päättää merkitykseltään laajakantoisista ja yhteiskunnallisesti merkittävistä periaatteista."

Laajemmin julkisen hallinnon palvelutuotantoon vaikuttavat pääosin Digi- ja väestötietoviraston hallinnoimat sähköisen asioinnin tukipalvelut, joista erityisesti sähköisen tunnistamisen palvelu muodostuu valtaosaan julkisen hallinnon palveluista solmukohdan, joten palveluja koskevilla häiriöillä on hyvin laajat haittavaikutukset viranomaisten palvelutuotantoon hallinnon asiakkaille. Hallinnon sähköisen asioinnin tukipalveluista annetun lain (571/2016, tukipalvelulaki) 19 § pitää sisällään vastaavan varautumissääntelyn kuin perustietotekniikkapalvelulain 15 §.

Julkisen hallinnon turvallisuusverkkotoiminnasta annetun lain (10/2015, turvallisuusverkkotoimintalaki) 1 §:n mukaan lain tarkoituksena on normaalioloissa ja niiden häiriötilanteissa sekä poikkeusoloissa varmistaa valtion ylimmän johdon ja yhteiskunnan turvallisuuden kannalta tärkeiden viranomaisten ja muiden toimijoiden yhteistoiminnan edellyttämän viestinnän häiriöttömyys ja jatkuvuus sekä turvata päätöksenteossa ja johtamisessa tarvittavan tiedon käytettävyys, eheys ja luottamuksellisuus. Lain 12 §:ssä on säädetty varautumisvelvollisuudesta niin normaaliolojen häiriötilanteisiin kuin poikkeusoloihin. Turvallisuusverkkotoimintalain tarkoituksena onkin estää häiriötilanteita myös poikkeusoloissa, joten kynnystä valmiuslain käytölle turvallisuusverkossa olevien häiriöiden vuoksi voidaan pitää erittäin korkeana.

Muista laajasti viranomaistoimintaan vaikuttavista säädöksistä voidaan nostaa esille sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annettu laki (784/2021), jonka 14 §:n 1 momentin mukaan sosiaali- ja terveydenhuollon valtakunnallisilla tietojärjestelmäpalveluilla on oltava tarpeelliset varajärjestelmät toimintahäiriöiden ja poikkeusolojen varalle.

Edellä mainituissa säädöksissä on perussääntelyä myös poikkeusoloihin varautumiseen. *Sääntely on jossain määrin epäselvä sen suhteen, miten poikkeusolot ymmärretään mainituissa säädöksissä suhteessa valmiuslakiin nähden, vaikka tukipalvelulaki sisältääkin monitulkintaisen viittaussäännöksen valmiuslakiin*. Tulevassa lainsäädännön kehittämistyössä tulisikin selkeyttää eri laeissa olevien poikkeusoloja koskevien säännösten sisältöä ja merkitystä.

Kaiken kaikkiaan normaaliolojen häiriötilanteita varten laadittu sääntely on hajanaista ja osin ohjausmalliltaan varsin sekavaa. Tällainen sääntely voi myös itsessään muodostua tehokkaan varautumisen sekä häiriötilanteissa tapahtuvan reagoinnin hidasteeksi tai esteeksi. *Selvää on, että hallinnon epäselvät rakenteet eivät voi toimia perusteena sille, että esimerkiksi tavanomaisissa tai laajoissakin kyberhyökkäystilanteissa jouduttaisiin turvautumaan poikkeusoloja varten laadittuun sääntelyyn*. Poikkeusolosääntely on tarkoitettu vain erittäin poikkeuksellisiin, ajallisesti pitkäkestoisiin ja vakaviin yhteiskunnan toiminnan vaarantaviin kriisitilanteisiin (PeVL 29/2022 vp). *Tästä syystä on syytä painottaa sitä, että viranomaisten varautuminen normaaliolojen vakaviinkin tietojärjestelmien häiriötilanteisiin tulee olla hyvin resursoitua ja että viranomaisilla on riittävät, täsmälliset ja tehokkaat toimivaltuudet normaaliolojen häiriötilanteista selviämiseen, mutta myös kybertoimintaympäristön seuraamiseen ja uhkien havaitsemiseen (ks. tästä myös HaVL7/2018 vp).*

Valmiuslainsäädännön tulevan kehittämisen yhteydessä on nähdäkseni välttämätöntä tehdä perusteellinen arvio tietojärjestelmiin kohdistuvista uhkatilanteista normaalioloissa sekä selkeyttää tietojärjestelmien palvelutuotantoon vaikuttavia viranomaisten toimivaltasuhteita sekä poikkeusoloihin varautumista ja poikkeusoloja koskevaa sääntelyä. Hallintovaliokunta onkin todennut (HaVL 30/2021 vp) varsin tuoreesti, että "viranomaisilla on oltava riittävät toimivaltuudet käyttää keinovalikoimaansa erilaisissa häiriötilanteissa ennakoivasti, nopeasti ja joustavasti. Riittävien toimivaltuuksien tulee olla käytettävissä jo normaalioloissa". *Merkitystä on myös sillä, että osa viranomaisten yhteisten tietojärjestelmäpalvelujen tuotannosta on annettu julkisomisteisten, mutta yksityisoikeudellisten yhtiöiden (kuten Erve Oy, Stuve Oy ja CSC Oy) hoidettavaksi ja merkittävä osa*

tietojärjestelmäpalveluista tuotetaan markkinoilla toimivissa yrityksissä tai niiden henkilökunnalla ostopalveluina. Tietojärjestelmien käyttöön ja toimintavarmuuteen liittyvä sääntely voi vaikuttaa myös tosiasiassa perusoikeuksien toteuttamiseen esimerkiksi perustuslain 21 §:ssä säädettyjen oikeusturvan ja hyvän hallinnon takeiden toteuttamiseen taikka 19 §:ssä säädettyyn oikeuteen saada riittäviä sosiaali- ja terveyspalveluja. Tämä painottaa sääntelyn ja toimivaltasuhteiden selkeän merkityksen ja täsmällisen sääntelyn tarvetta.

Hallituksen esitys on valmisteltu kiireellä eikä kaikkia hyvään lainvalmistelutapaan liittyviä seikkoja ole toteutettu valmistelussa. Hallituksen esityksen mukaan valmisteluaikataulu ei ole mahdollistanut säännösten kokonaisvaltaista tarkastelua. *Nähdäkseni on selvää, että valmiuslain kokonaisuudistuksessa on tehtävä huolellinen arviointi siitä, missä tilanteissa valmiuslakia voitaisiin yleensäkin soveltaa, kun kysymys on tietojärjestelmiin tai tietoverkkoihin kohdistuvista kyberuhista tai kyberhyökkäyksistä. Tällainen toiminta on kuitenkin valitettavasti normaalioloihin kuuluvaa viranomaistoimintaa häiritsevää/haittaavaa toimintaa, jota pitää pystyä torjumaan normaaliolojen toimivaltuuksilla ja menettelyillä.*

2. Poikkeusolojen määritelmä

Hallituksen esityksen 1. lakiehdotus sisältää valmiuslain poikkeusolojen määritelmäsäännöksen pelkistetyn säännösmuutosehdotuksen, jossa varsinainen sääntely on luettavissa hallituksen esityksen perusteluista. *Tällaista erityisesti perusoikeuksien rajoittamiseen ja hallinnon toimintaan liittyvää sääntelymallia ei voida pitää hyväksyttävänä, koska varsinaisesta säännöksestä on pystyttävä suoraan toteamaan säännöksen sisältö, merkitys ja laajuus ts. se mistä säädetään. Perusteluilla säätämistä* ei voida pitää perustuslain 2 §:n 3 momentissa säädetty huomioon ottaen ongelmattomana, koska julkisen vallan käytön on perustuttava laissa säädettyyn ja julkisessa toiminnassa on noudatettava tarkoin lakia. *Hallinnon lainalaisuus ja lakisidonnaisuuden vaatimus tarkoittavat lainvalmistelussa pidättäytymistä perusteluissa säätämisestä.* Niin ikään perusoikeuksien rajoitusperusteisiin kuuluvat sääntelyn täsmällisyyden ja tarkkarajaisuuden vaatimukset edellyttävät lain säännöstasolta todennettavissa olevaa sääntelyä.

Hallituksen esityksen 1. lakiehdotuksen 3 §:än ehdotetaan lisättäväksi poikkeusolojen määritelmään uusi 6 kohta, jonka mukaan poikkeusoloja olisivat valmiuslain mukaan muu julkisen vallan päätöksentekokykyyn, yhteiskunnan kriittisen infrastruktuurin toimivuuteen, rajaturvallisuuteen tai yleiseen järjestykseen ja turvallisuuteen kohdistuva uhka, toiminta, tapahtuma tai näiden yhteisvaikutus, joka erityisen vakavasti ja olennaisesti vaarantaa kansallista turvallisuutta, yhteiskunnan toimintakykyä tai väestön elinmahdollisuuksia. *Ehdotettu määritelmä on osin päällekkäinen määritelmän muiden kohtien kanssa ja sisällöllisesti varsin avoin ja epätäsmällinen.*

Uutta kohtaa on avattu perusteluissa, joiden mukaan uusi määritelmä ”mahdollistaisi täyttyessään rajatusti valmiuslain käyttöönoton ja sen toimivaltuuksien aktivoinnin myös hybridiuhkien ja muiden kansallista turvallisuutta, yhteiskunnan toimintakykyä tai väestön elinmahdollisuuksia erityisen vakavasti ja olennaisesti vaarantavien uhkien johdosta. Tarkoituksena on varmistaa viranomaisten mahdollisuudet vastata valmiuslain nykyisiä poikkeusoloperusteita kattavammin tehokkaasti ja oikeasuhtaisesti vallitsevan yhteiskunnallisen tilanteen mukaisiin turvallisuusuhkiin”. *Peruslähtökohdiltaan perusteluissa esitetty tavoite on kannatettava ja välttämätönkin.*

Hallintovaliokunta on eri yhteyksissä käsitellyt hybridivaikuttamista ja siihen liittyviä sääntelykysymyksiä (HaVM 5/2017 vp, HaVL 7/2018 vp, HaVL 30/2021 vp). Hallituksen esityksessä todetaan, että määritelmä käsittäisi erityisesti hybridiuhkien vakavimmat ilmenemismuodot. Hallintovaliokunta on käsitellyt aiemmin hybridiuhkien sisältöä. Hallintovaliokunnan (HaVL 5/2017 vp) mukaan hybridiuhkan käsitteellä tarkoitetaan erilaisia turvallisuutta vaarantavia ja yhteiskuntaa haavoittavia toimia (poliittisia, diplomaattisia, sotilaallisia, taloudellisia, informatiivisia, teknologisia tai infrastruktuuriin vaikuttavia toimenpiteitä). Tässä suhteessa valmiuslakiin ehdotetut vakavimmat ilmenemismuodot ilmenevät säännöksestä vain osittain. Säännöksestä ei käy ilmi selkeästi yhteiskunnan ja erityisesti julkisen hallinnon

käyttämään tieto- ja viestintäteknologiaan liittyvät uhat tai toiminta, joka voisi olla perusteena joissakin tilanteissa poikkeusoloja koskevan sääntelyn käyttöönotolle. Perusteluissa kylläkin todetaan, että määritelmän mukaisessa tilanteessa ”Kyse voisi olla esimerkiksi päätöksenteon kannalta tärkeisiin tieto- ja viestintäteknisiin palveluihin sekä tietojärjestelmiin kohdistuvasta häirinnästä, tietomurroista, haitta- tai vakoiluohjelmien levittämisestä, palvelunestohyökkäyksistä taikka äänestys- tai vaalituloksen manipuloinnista”.

Nähdäkseni tietojärjestelmiä ja tietoverkkoja koskevilta osin ehdotettu sääntely on ainakin osittain rinnakkaista tai päällekkäistä valmiuslain 3 §:n 3 kohdan kanssa. Perustuslakivaliokunta on aikaan todennut, että esimerkiksi tieto- ja viestintäjärjestelmiin kohdistuvat erityisen vakavat hyökkäykset voivat muodostaa lain 3 §:n 3 kohdassa tarkoitetun poikkeusolon (PeVL 6/2009 vp).

Kokonaisarviona totean, että tietojärjestelmiin ja tietoverkkojen toimintaan liittyvillä syillä *ei voida ehdotetun sääntelyn perusteella yksin perustella poikkeusoloihin siirtymistä ja valmiuslain toimivaltuuksien käyttöönottoa*. Palvelunestohyökkäyksiä, haitta- ja vakoiluohjelmia, tietomurtoja, tietoliikennehäirintää tai tietojärjestelmien häirintää tapahtuu jatkuvasti ja päivittäin normaalioloissakin. Jotta tietojärjestelmiin ja tietoverkkoihin liittyvillä syillä voitaisiin perustella valmiuslain eräiden toimivaltasäännösten aktivointia, tulisi tällaisilla häiriöillä olla *pitkäkestoinen, erittäin laaja sekä perusoikeuksien toteuttamista merkittävästi haittaava vaikutus*. T*ässä suhteessa ehdotettua määritelmää tulisi tarkentaa tieto- ja viestintäteknologisten uhkien osalta* sekä korostaa, että näihin kohdistuvat uhkat ja haittaavat toimenpiteet voivat olla perusteena nimenomaisesti hybridiuhkatilanteissa, joissa yhteiskuntaan kohdistuu samanaikaisesti useita viranomaisten toimintaa haittaavia tai estäviä toimia, joita ei voitaisi torjua tai rajoittaa normaaliolojen toimivaltasäännöksillä. *Hallituksen esityksen perustelut ovat liian yleisellä tasolla, jolloin myöskään niistä ei saada riittävää kuvaa siitä, missä tilanteessa poikkeusolojen määritelmää voitaisiin soveltaa tietojärjestelmiin ja tietoverkkoon kohdistuvien kyberuhkien tai -hyökkäysten tilanteissa vai voidaanko lainkaan.*

3. Kriittinen infrastruktuuri

Hallituksen esityksen 1. lakiehdotuksen 3 §:n 6 kohtaan ehdotetaan otettavaksi yhteiskunnan kriittisen infrastruktuurin käsite. Lakiehdotus ei kuitenkaan sisällä yhteiskunnan kriittisen infrastruktuurin määritelmää, joten käsite ja käytännössä myös peruste poikkeusoloihin siirtymiselle jää säännöksen perusteluissa esitetyn varaan.

Säännöksen perustelujen mukaan yhteiskunnan kriittiseen infrastruktuuriin sisältyisi myös eräät tietojärjestelmä- ja tietoverkkopalvelut. Hallituksen esityksen mukaan ”kriittiseen infrastruktuuriin kuuluvat myös edellä tarkoitettujen toimintojen ylläpitämisen ja jatkuvuuden turvaamisen kannalta välttämättömät tieto- ja viestintätekniset palvelut sekä tietojärjestelmät. Tällaisia olisivat myös ylimpien valtioelinten työskentelyn ja valtion johtamisen sekä ihmisten terveydestä ja turvallisuudesta vastaavien viranomaisten päätöksenteko- ja toimintakyvyn mahdollistavat tieto- ja viestintätekniset palvelut sekä tietojärjestelmät”. Edelleen hallituksen esityksen mukaan ”Yhteiskunnan elintärkeiden toimintojen keskinäisriippuvuudesta johtuen kriittinen infrastruktuuri on yhä alttiimpi tietoverkkojen välityksellä toteutettavalle sabotaasille ja kokonaisvaltaiselle lamauttamiselle. Kriittisen infrastruktuurin toimivuuteen kohdistuvissa uhkissa saattaisi siten olla kyse paitsi edellä tarkoitettujen toimialojen tuotanto- ja jakeluketjujen ennakoimattomasta, laajamittaisesta ja pitempiaikaisesta keskeytymisestä tai niihin kohdistuvista muista vakavista häiriöistä, myös näitä toimintoja ylläpitävien tietojärjestelmien kaatumisesta tai niihin tunkeutumisesta, tietoliikenteen merkittävästä kuormittamisesta, tietojärjestelmien käytön estämisestä tai niihin pääsyn estymisestä, tietovarastoihin tunkeutumisesta tai niiden sisältämien tietojen käytön estämisestä, muuttamisesta tai tuhoamisesta taikka näihin rinnastuvista vakavista häiriöistä. Myös kriittisen infrastruktuurin toimintaan kohdennettavalla verkkohyökkäyksellä uhkaamista voitaisiin pitää säännöksessä tarkoitettuna uhkana, jos se olisi mittakaavaltaan ja vaikutuksiltaan riittävän vakava.”

Hallituksen esityksestä jää epäselväksi, missä kulkee raja normaalioloissa tapahtuvien tahallisesti tuotettujen häiriötilanteiden ja poikkeusoloihin johtavien häiriötilanteiden välillä. Koska valmiuslaki tarkoittaa viranomaisille poikkeuksellisten toimivaltuuksien myöntämistä ja perusoikeuksiin puuttumista, tulisi sääntelyn olla täsmällistä ja sellaista, joka muodostaa selkeän kynnyksen sille, millaisissa kyberuhkatilanteissa tai kyberhyökkäyksissä olisi käsillä poikkeusoloja koskevan sääntelyn käyttöönottomahdollisuus. Kuten hallintovaliokunta on todennut (HaVL 7/2018 vp), että useimpien valtioiden sotilaalliseen varautumiseen liittyy valmius tietojärjestelmien häirintään, hyväksikäyttöön ja tuhoamiseen. *Nähdäkseni valmiuslain aktivointi tietojärjestelmiä ja tietoverkkoja uhkaavissa tilanteissa voisi tulla kysymykseen esimerkiksi sotilaallisissa kyberhyökkäystilanteissa, jos tällaista uhkatilannetta käytettäisiin yksin perusteena poikkeusoloihin siirtymiselle.*

Edelleen on syytä korostaa, että viranomaisilla tulee olla selkeästi laissa säädetyt velvollisuudet varautua kyberuhkiin sekä ylläpitää kyvykkyyttä kyberhyökkäyksiä varten. Julkisen hallinnon tiedonhallinnasta annettu laki (906/2019, tiedonhallintalaki) ohjaa ja velvoittaa yleispiirteisellä sääntelyllä viranomaisia varautumaan uhkiin sekä ylläpitämään kyvykkyyttä uhkien torjumiseksi. Tiedonhallintalain sääntely ei ole kuitenkaan tarpeeseensa nähden riittävän täsmällistä. *Viranomaisten kyvykkyyksien puutteet eivät voi olla perusteena yhteiskunnan ajautumisessa poikkeusoloihin.*

4. Normaaliolojen toimivaltasuhteet suhteessa poikkeusoloihin

Tuon myös esille hallituksen esitykseen liittyvän ja erityisesti viranomaisten toimivaltasuhteisiin vaikuttavan epäsuhdan normaaliolojen ja poikkeusolojen tietojärjestelmiin ja tietoverkkoihin liittyvien ohjausmekanismien välillä.

Valmiuslain 9 luvussa säädetyt toimivaltuudet tietojärjestelmien ja tietoverkkojen osalta kuuluvat pääosin liikenne- ja viestintäministeriölle sekä joiltakin osin työ- ja elinkeinoministeriön alaiselle hallinnolle. Poikkeuksen tähän tekee valtionhallinto. Valmiuslain 105 §:n mukaan valtiovarainministeriö voi määrätä poikkeusoloissa valtion tietohallinnon, tiedonkäsittelyn, sähköisten palveluiden, tietoliikenteen ja tietoturvallisuuden järjestämisestä. Valtiovarainministeriön ohjaus ei koske kuitenkaan puolustusvoimien, rajavartiolaitoksen, poliisin, pelastusviranomaisten ja hätäkeskusten toiminnallisia tietojärjestelmiä. Siten valtiovarainministeriön toimivalta ulottuu ainoastaan rajattuun osaan valtionhallintoa ja toisaalta toimivaltasääntely ei ulotu muuhun julkiseen hallintoon, vaan muu julkinen hallinto, kuten kunnat, hyvinvointialueet ja itsenäiset julkisoikeudelliset laitokset, jäävät valtiovarainministeriön poikkeusoloja koskevan toimivaltasäänttelyn piiriin ulkopuolelle, joten ne kuuluvat valmiuslain 9 luvun piirin. Toisaalta turvallisuusverkkotoiminnasta annetussa lain 14 §:ssä valtiovarainministeriöllä on toimivaltuuksia, jotka ilmeisesti ulottuisivat poikkeusoloissakin valmiuslain 105 §:n 2 momentissa tarkoitettuihin turvallisuusviranomaisiin.

Valtioneuvoston ohjesäännön (262/2003) 12 §:n 7 kohdan mukaan valtioneuvoston kanslian toimialaan kuuluvat valtioneuvoston yhteinen tilannekuva, varautuminen ja turvallisuus, häiriötilanteiden hallinnan yleinen yhteensovittaminen ja 9 kohdan mukaan valtioneuvoston ja sen ministeriöiden yhteinen tietohallinto, mukaan lukien ulkoasiainhallinnon ulkomaanedustustojen tieto- ja viestintätekniset peruspalvelut, ja asiakirjahallinto sekä niihin liittyvä hyvän tiedonhallintatavan ja yhteentoimivuuden ohjaus, kehittäminen ja yhteensovittaminen sekä arkistonmuodostajan tehtävät ja 10 kohdan mukaan valtioneuvoston ja sen ministeriöiden yhteisen verkkopalvelun ja sisäisen verkkoviestinnän kehittäminen ja yhteensovittaminen. Valtioneuvoston ohjesäännön 17 §:n 11 kohdan mukaan valtiovarainministeriön toimialaan kuuluvat julkisen hallinnon tietopolitiikan, tiedonhallinnan ja sähköisen asioinnin yleiset perusteet. Tiedonhallinta sisältää myös tietoturvallisuuden. Valtiovarainministeriölle on säädetty myös

varautumiseen ja poikkeusoloihin liittyviä tehtäviä ja niihin liittyvää toimivaltaa perustietotekniikkalaissa, tukipalvelulaissa ja turvallisuusverkkotoimintalaissa.

Kaiken kaikkiaan normaaliolojen ohjausjärjestelmä ei ole edes valtioneuvostotasolla selvää. Varsinainen ministeriötasoinen toimivaltasääntely julkisen hallinnon tietohallintoon tai tiedonhallintaan normaaliolojen kyberturvallisuusuhkien varautumiseksi tai kyberuhkien torjunnan johtamiseksi on hyvin vähäistä.

Liikenne- ja viestintävirastossa toimiva kyberturvallisuuskeskus kerää tilannetietoa kyberuhista, tiedottaa niistä ja antaa kyberuhkiin varautumiseen sekä torjuntaan asiantuntijaneuvontaa. Julkisen hallinnon tiedonhallintalautakunta puolestaan informaatio-ohjaa tiedonhallintalain puitteissa valtion, kuntien ja hyvinvointialueiden tietoturvallisuustoimenpiteiden kehittämistä, mutta ei koko julkista hallintoa. Digi- ja väestötietovirastolle (DVV) on säädetty asetuksentasoisina tehtävinä (asetus 53/2020) 1) tuottaa ja kehittää julkisen hallinnon tietoturvallisuutta koskevia menetelmiä ja välineitä; 2) tuottaa tietoturvallisuutta koskevia asiantuntijapalveluja valtionhallinnolle ja 3) ylläpitää yleistä tilannekuvaa julkisen hallinnon tietoturvallisuudesta. DVV:llä ei ole kuitenkaan tehtävien hoitoon liittyvää toimivaltasääntelyä, joten asetuksentasoisina ilman toimivaltaa sisältävinä tehtävinä ne eivät ole nykyisessä toimintaympäristössä merkityksellisiä tai vaikuttavia.

Edellä esitetyn perusteella pidän tarpeellisena, että osana valmiuslain kokonaisuudistamista tehtäisiin myös kokonaisarvio normaaliolojen julkisen hallinnon varautumisorganisaation toiminnasta ja sääntelystä. Lähtökohtana voidaan pitää sitä, että tietojärjestelmien ja tietoverkkojen toimintaan liittyvät uhat voidaan hallita ja torjua normaaliolojen lainsäädännön ja siihen liittyvien selkeiden ja vaikuttavien toimivaltasäännösten puitteissa. Kuten edellä on mainittu, lähinnä sotilaalliset kyberhyökkäykset voisivat muodostaa tilanteen, jossa olisi tarvetta käyttää valmiuslain poikkeusoloja koskevaa sääntelyä, joskin sitäkin tulisi kehittää valmiuslakiin siten, että valmiusorganisaatio vastaisi myös tieto- ja viestintäteknisten järjestelmien ohjauksessa normaaliolojen ohjausrakenteita. Nykyinen valmiuslain sääntely ei tue tällaista julkisen hallinnon ohjausta ja on omiaan heikentämään kykyä reagoida poikkeusolojen uhkatilanteisiin poikkeavalla ohjausjärjestelmärakenteellaan.

Vantaalla 31.5.2022

Tomi Voutilainen
julkisoikeuden professori, dosentti