Yrityslainsäädäntö
Markku Rajamäki

Eduskunnan talousvaliokunnalle
TaV@eduskunta.fi

Muistio 1 (4)

21.10.2025

Viite: Talousvaliokunta torstai 23.10.2025 klo 12.00 / VNS 6/2025 vp / Asiantuntijapyyntö 14.10.2025

Elinkeinoelämän keskusliitto EK:n asiantuntijalausunto VNS 6/2025 vp Valtioneuvoston Sisäisen turvallisuuden selonteosta

Kiitämme lausuntomahdollisuudesta. Otamme tässä lausunnossa kantaa selontekoon vain valiokunnan pyytämiltä osin eli koskien kriittisen infrastruktuurin suojaamista koskevaa lukua 3.7 sekä siihen liittyviä toimenpide- ja kehittämislinjauksia.

Yleisesti toteamme, että selonteon haaste on jossain määrin se, että monessa kohdin esitetään toimenpiteenä viranomaisten toimivaltuuksien ja tiedonvaihdon kehittämistä, mutta ei avata, miten nykyinen lainsäädäntö estää sen tai on puutteellinen, ja miten sitä näistä syistä tulisi muuttaa. Tämä vaikeuttaa kannanottamista yksittäisiin toimenpiteisiin ja linjauksiin. Monet toimenpiteet koskevat herkkiä asioita, joissa punninnan kohteina ovat toisaalta viranomaisten tietotarpeet, toisaalta kohdehenkilöiden ja toimenpiteestä riippuen laajempienkin henkilöjoukkojen yksityisyyden suoja.

Luku 3.7 Suomi suojaa kriittistä infrastruktuuriaan

Olemme yhtä mieltä siitä, että kriittisen infrastruktuurin suojaamista tulee entisestään kehittää.

Koska kaikkea ei ole mahdollista ennalta estää, kriittisen infrastruktuurin suojauskysymysten osalta tulee kiinnittää huomiota myös korjauskapasiteetteihin, esim. merenalaisten kaapeleiden korjausaluksiin ja -välineistöön. Kapasiteetit ovat monilta osin myös kansainväliseen yhteistyöhön ja yhteisten tarpeiden ratkaisemiseen liittyvä kysymys. Sen vuoksi onkin hyvä, että asiasta on jo myös EU-tasolla aloite etenemässä.

Varautumisen keskeisin raaka-aine on tieto, tarkemmin analysoitu tilannekuvatieto jatkokehitysarvioineen. Luku keskittyy tässä suhteessa liiaksi viranomaisten tiedontarpeisiin ja tiedonvaihtoon. Suomen kriittinen infrastruktuuri on valtaosin yksityisten yritysten omistuksessa, hallinnassa ja operoinnissa. Kun puhutaan hybridivaikuttamisesta, kriittisen

infrastruktuurin toimijat ovat vaikuttamisen maaleja. Sen vuoksi tulisi koko ajan miettiä, miten huolehdimme nykyistä paremmin siitä, että ei pelkästään viranomaisilla, vaan myös kriittisen infrastruktuurin yrityksillä on yhteinen tilannekuva viranomaisten kanssa. Viranomaisten tiedonkulusta huolehtiminen ei ole riittävää. Parempi tiedonkulku osaltaan parantaisi myös yritysten mahdollisuuksia huolehtia alihankintaketjuihinsa liittyvistä riskeistä.

Tiedonvaihto on tärkeää myös muiden selonteon osa-alueiden kannalta, mm. järjestäytyneen ja vakavan rikollisuuden, tietoverkkoavusteisten rikosten torjunnan sekä vieraiden valtioiden vakoilun torjunnan näkökulmasta.

Tietoon ja tiedonvaihtoon liittyy myös se, että tiedon huoltovarmuutta tulisi korostaa selonteossa enemmän sekä yleisesti että myös kriittisen infrastruktuurin suojaamiseen liittyen, erityisesti kriittistä infrastruktuuria koskevissa poikkeus- ja kriisitilanteissa. Tiedon huoltovarmuus toteutuu vain, kun kaikki kriittiset tiedontarpeessa olevat toimijat (ml. elinkeinoelämä) ovat tiedonjaon piirissä.

Luvussa todetaan myös, että "Sisäisen turvallisuuden viranomaisten havainnointi- ja vastatoimintakykyä muun muassa droonien osalta tuleekin edelleen kehittää". Tämä on varmasti totta, mutta ei riittävää. Lainsäädäntömme ei ole droonien torjunnan osalta osin ajan tasalla. Sähköisen viestinnän palveluista annettu laki ja muu asiaan liittyvä lainsäädäntö tulisi ottaa miehittämättömien ilma-alusten (droonien) torjunnan osalta uuteen tarkasteluun. Kriittisten kohteiden yksityisillä toimijoilla tulisi olla nykyistä paremmat mahdollisuudet myös itsenäiseen ilma-alusten torjuntaan. Torjunta ei jatkossakaan voi olla vain viranomaisten varassa.

Luvussa on mainittu myös CER-direktiivin toimeenpano. Ennen kuin harkitaan uusia toimenpiteitä tai lainsäädäntöä, CER-direktiivin toimeenpanon osalta on keskeistä varmistaa eri valvontaviranomaisten valvontatoimien yhdenmukaisuus, missä työssä sisäministeriön rooli on keskeinen. Direktiivin ja sen toimeenpanolain vaatimukset on kuvattu hyvin ylätasoisesti ja tarkempi sanoitus vaatimusten sisällölle annetaan käytännön valvontatoiminnassa.

Kyberturvallisuuden osalta selonteko ei riittävästi tunnista yksityisten yritysten roolia kyberturvallisuuden varmistamisessa, vaan keskittyy lähes yksinomaan viranomaisten tilannejohtamiseen tilanteessa, jossa häiriö on jo realisoitunut. Suomessa lähes kaikki kriittinen infrastruktuuri on kiinnittynyt tietojärjestelmiin. Kyberturvallisuuden riskienhallintatoimenpiteiden keskeinen vastuu on yrityksillä ja yhteisöillä, sillä ne muodostavat suurimman osan yhteiskunnan toiminnallisesta ja taloudellisesta rakenteesta sekä omaavat juridis-hallinnollis-teknologiset kyvyt niiden toteuttamiseen. Yritykset ja yhteisöt tunnistavat tieto- ja

viestintäjärjestelmiinsä kohdistuvat poikkeamat, selvittävät niiden syyt ja vaikutukset sekä poistavat kielteiset vaikutukset.

Toimenpiteet ja linjaukset
Kriittistä infrastruktuuria koskevien selonteon toimenpiteiden ja linjausten osalta haluamme painottaa seuraavia:

3. Suojataan Suomelle kriittistä infrastruktuuria.

Uudistetaan turvallisuusselvityslakia. Tunnistetut säädösmuutostarpeet kohdistuvat muun muassa selvitysten laatimisessa käytettäviin tietoihin ja tietolähteisiin, nuhteettomuuden seurantaan ja viranomaisten väliseen tiedonvaihtoon. Lisäksi arvioidaan ja määritellään uudelleen henkilöturvallisuusselvitysten piiriin kuuluvat tehtävät ja henkilöturvallisuusselvitysten laajuus tehtäväkohtaisesti.

Kannatamme turvallisuusselvityslain uudistamista. Mainittujen lisäksi tulisi pohtia:
- Merkityksellisten tietojen antaminen myös kohdehenkilön työnantajalle tilanteessa, jossa jokin toinen organisaatio, esim. asiakkaana toimiva viranomainen on toiminut selvityksen hakijana. Nykyinen laki kieltää tämän, vaikka samaan aikaan kesällä 2025 voimaan tullut satamia koskeva muutos oikeuttaa hakijana olevan satamanpitäjän ilmoittamaan merkitykselliset tiedot henkilön työnantajalle, esim. satama-alueella operoivalle lastinkäsittely-yritykselle.
- Selvitysmenettelyyn hyväksyttyjen yritysten mahdollisuus pääsyyn turvallisuusselvitysrekisteriin niin, että ne näkisivät, onko henkilöllä jo voimassa oleva turvallisuusselvitys ja jos on, nykyistä nopeampi ja suoraviivaisempi prosessi liittyä olemassa olevaan turvallisuusselvitykseen. Nyt eri vaiheissa tehdään paljon turhaa työtä, kun näkyvyyttä ei ole.
- Nykyisen lain selventäminen niin, että jatkossa sen tulkintaan ei tarvittaisi arviointikriteerilautakuntaa.

Panostetaan kriittisen infrastruktuurin kohteiden suojaamiseen CER-direktiivin toimeenpanon edellyttämällä tasolla. Arvioidaan energia- ja vesi-infrastruktuurin rakenteellisen suojaamisen sekä jatkorakentamisessa maanalaisen rakentamisen tarvetta sekä tehdään tarvittavat toimenpiteet.

CER-direktiivin toimeenpanon osalta nyt on keskeistä varmistaa valvontaviranomaisten yhdenmukaiset tulkinnat

ja käytännöt kaikilla valvontasektoreilla. Sisäministeriön rooli on tässä keskeinen.

Arvioidaan merialueilla olevan kriittisen infrastruktuurin ylläpidon ja suojaamisen haasteet sekä näiden edellyttämä lainsäädännöllinen, valvonnallinen ja teknologinen vaste eri sisäisen turvallisuuden viranomaisten osalta.

Kannatamme toimenpidettä. Painotamme kuitenkin sitä, että koska kaikkia vihamielisiä kriittiseen infrastruktuuriin kohdistuvia tekoja ei ole mahdollista estää ennalta, eikä kriittistä infrastruktuuria ole mahdollista tässä tarkoituksessa aukottomasti valvoa, on tärkeää keskittyä sekä kehittämään kriittisestä infrastruktuurista entistä iskunkestävämpää ja samaan aikaan kehittää ja ylläpitää kriittiseen infrastruktuuriin liittyviä korjauskyvykkyyksiä kansallisesti, mutta myös kansainvälisessä yhteistyössä.