TURUN YLIOPISTO
Oikeustieteellinen tiedekunta

Sähköverkkojen kyberturvallisuussääntely

Kriittisten toimialojen varautuminen kyberuhkiin

Normaaliolojen häiriötilanteiden ja poikkeusolojen sääntely

OTM-opinnäytetyö

Laatija:
Lasse Heliste

16.3.2023

TURUN YLIOPISTO
Oikeustieteellinen tiedekunta

Tiivistelmäsivu

OTM-opinnäytetyö

Oppiaine: Oikeustiede
Tekijä: Lasse Heliste
Otsikko: Sähköverkkojen kyberturvallisuussääntely – Kriittisten toimialojen varautuminen kyberuhkiin
Ohjaajat: Antti Aine, Veli-Pekka Nurmi
Sivumäärä: 80 sivua
Päivämäärä: 16.3.2023

Sähköverkot ovat elintärkeitä koko yhteiskuntamme toiminnalle. Sähköverkonhaltijat nojaavat tänä päivänä toiminnassaan paljolti digitaalisiin tietojärjestelmiin ja viestintäverkkoihin, joten järjestelmien kyberturvallisuudesta huolehtiminen on tullut entistä tärkeämmäksi. Jokin vihamielinen taho voi pyrkiä esimerkiksi ujuttamaan haittaohjelman verkonhaltijan tietojärjestelmiin, ja sitä kautta lamauttamaan sähkönjakelun. Olisikin tärkeää, että lainsäädännöstämme löytyisivät asianmukaiset ja kattavat säännökset, joilla sähköverkonhaltijat velvoitettaisiin huolehtimaan organisaationsa kyberturvallisuudesta.

Tässä tutkielmassa kartoitetaan sähköverkonhaltijoiden kyberturvallisuussääntelyä, arvioidaan sen toimivuutta ja esitetään siihen parannuksia. Tutkimusmetodeina käytetään lainopillista tutkimusta sekä de lege ferenda -tyylistä pohdintaa. Tutkimuksessa kartoitetaan sähköverkonhaltijoiden kyberturvallisuuteen liittyvää velvoitesääntelyä sekä viranomais-, valvonta- ja sanktiosääntelyä. Lisäksi tutkielmassa käsitellään valikoivasti muiden kriittisten toimialojen vastaavaa sääntelyä ja verrataan tätä sähköverkkojen sääntelyyn. Lopuksi esitetään kehitysehdotuksia vallitsevaan oikeustilaan lainopillisen tutkimuksen, oikeuskirjallisuuden sekä viranomaislähteiden perusteella.

Tutkimuksessa esitetään, että nykyinen sähköverkkojen kyberturvallisuuteen liittyvä EU-tasoinen sekä kansallisen lain tasoinen sääntely on hyvin yleisluonteista, eikä siitä voida siksi johtaa konkreettisia ja tehokkaita riskienhallintavelvoitteita. Lisäksi tutkimuksessa tuodaan esille, että toisin kuin monilla muilla kriittisillä toimialoilla, Energiavirastolla alan valvovana viranomaisena ei ole tällä hetkellä oikeutta antaa kyberturvallisuusvelvoitteisiin liittyen lakia täsmentäviä määräyksiä.

Tutkielmassa tuodaan myös ilmi, että Energiaviraston toimivaltuudet, jotka liittyvät sähköverkonhaltijoiden kyberturvallisuusvelvoitteiden noudattamisen valvontaan, ovat nykyisellään jossain määrin epäselviä. Lisäksi velvoitteiden laiminlyömisestä seuraaviin sanktioihin liittyvä sääntely on puutteellista. Tutkielmassa argumentoidaan, että Suomi ei ole onnistunut implementoimaan kunnolla EU-sääntelystä johtuvia velvoitteita kaikille kriittisille toimialoille, kuten energiahuoltoon. Toisaalta joillakin toimialoilla, kuten digitaalisen infrastruktuurin alalla, finanssimarkkinoilla sekä terveydenhuollossa, vallitseva oikeustila vaikuttaa olevan selvästi parempi.

Tutkielmassa esitetään useita parannuksia sähköverkonhaltijoiden kyberturvallisuussääntelyyn. Parannusehdotukset koskevat esimerkiksi entistä kattavampia ja yksityiskohtaisempia riskienhallintavelvoitteita, toimijoiden velvollisuutta säännöllisten tietoturva-auditointien teettämiseen, velvollisuutta yleisesti tunnustettujen tietoturvasertifikaattien hankkimiseen, sekä selkeää velvoitetta dokumentoida kyberturvallisuuden hallintatoimenpiteet. Lisäksi esitetään, että Energiaviraston valvontatoimivaltuutta tulisi lainsäädännössä selkeyttää ja sille tulisi säätää valtuudet antaa lakia tarkentavia määräyksiä. Energiavirastolla tulisi myös olla mahdollisuus määrätä tehokkaita sanktioita, kuten hallinnollisia sakkoja sähköverkonhaltijoille, jotka ovat laiminlyöneet kyberturvallisuusriskien hallintaan liittyvät velvoitteensa.

Avainsanat: sähköverkot, kyberturvallisuus, kyberturvallisuussääntely, kriittiset toimijat, varautuminen

Sisällys

Lähteet

Kirjallisuus

Aine, Antti – Nurmi, Veli-Pekka – Ossa, Jaakko – Penttilä, Teemu – Salmi, Ilkka – Virtanen, Vesa, Moderni Kriisilainsäädäntö. WSOYpro Oy 2011.

Aine, Antti – Nurmi, Veli-Pekka – Valtonen, Vesa, Oikeuden resilienssi, perusoikeudet ja kokonaisturvallisuus. Lakimies 6/2022, s. 841–873.

Bayuk, Jennifer L. – Healey, Jason – Rohmeyer, Paul – Sachs, Marcus H. – Schmidt, Jeffrey – Weiss, Joseph, Cyber Security Policy Guidebook. John Wiley & Sons, Inc. 2012.

Calder, Alan, Network and Information Systems (NIS) Regulations – A pocket guide for operators of essential services. IT Governance Publishing Ltd 2018.

Carter, Candice, Critical Infrastrucure and Cyber Security. Imperva 2017. (https://www.imperva.com/blog/critical-infrastructure-cyber-security/, Luettu 31.5.2022).

Chałubińska-Jentkiewicz, Katarzyna – Radoniewicz, Philip – Zieliński, Tadeusz, Cyber Security in Poland – Legal Aspects. Springer 2022.

European Telecommunications Standards Institute (ETSI), Technical Report, CYBER; Implementation of the Network and Information Security (NIS) directive, ETSI TR 103 456 V1.1.1 (2017-10).

Helsingin seudun kauppakamari, Yrityksiin kohdistuvat kyberuhat 2019 – Kolmas aiheesta tehty selvitys – Yritysten tietoverkkoon kohdistuvat tunkeutumiset 2019.

Hyppönen, Mikko, Internet. WSOY 2021.

Hämäläinen, Mika, Suomi sähköomavaraiseksi – Fingrid ottaa etunojaa. Tekniikan maailma 22/2021, s. 66–71.

Iivanainen, Tuomas, ISO/IEC 27001 -tietoturvasertifikaatin kokonaiskustannukset, Liiketalouden koulutusohjelma. Satakunnan ammattikorkeakoulu 2019.

Lahti, Ville, Liikennejärjestelmän verkko- ja tietojärjestelmien turvallisuuden sääntely. Jyväskylän yliopisto, Informaatioteknologian tiedekunta 2022.

Lonka, Harriet – Limnéll, Jarno, Strategiasta käytäntöön: Suomi kyberlainsäädäntöä kehittämässä. Oikeus 2015 (44), 2: 202–213.

Maxwell, Winston J. – Bourreau, Marc, Technology Neutrality in Internet, Telecoms and Data Protection Regulation. Thomson Reuters (Professional) UK Limited and Contributors 2014.

Michalec, Ola – Milyaeva Sveta – Rashid Awais, Reconfiguring governance: How cyber security regulations are reconfiguring water governance. Regulations & Governance 2022, 16, 1325–1342.

Mykkänen, Pekka, Ruotsin viranomaiset: Nord Stream -putkien räjähdykset olivat ”törkeä sabotaasi”. Helsingin sanomat (https://www.hs.fi/ulkomaat/art-2000009210474.html, Luettu 24.12.2022).

Mäenpää, Olli, Hallinto-oikeus. Alma Talent, Helsinki 2018.

Perez, Evan, First on CNN: U.S. investigators find proof of cyberattack on Ukraine power grid. CNN (https://edition.cnn.com/2016/02/03/politics/cyberattack-ukraine-power-grid/index.html, Luettu 4.12.2021).

Pöyhönen, Jouni, Standardit, ohjeet ja suositukset osana teollisuusorganisaatioiden kyberturvallisuuden hallintaa: CIRP-raportti 2017. Jyväskylän yliopisto, Informaatioteknologian tiedekunnan julkaisuja / Jyväskylän yliopisto 2018, 55.

Pöyhönen, Jouni, Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa – Systeemiajattelu. JYU Dissertations 270, 2020.

Pöyhönen, Jouni, – Lehto, Martti, Cyber security creation as part of the management of an energy company, ECCWS 2017: Proceedings of the 16th European Conference on Cyber Warfare and Security, s. 332–340. Academic Conferences and Publishing International Limited 2017.

Raitio, Juha – Tuominen Tomi, Euroopan unionin oikeus. 2., uudistettu painos. Alma Talent Oy 2020.

Sales, Nathan Alexander, Regulating Cyber-security. Northwestern University Law Review, Vol. 107, No. 4, 2013.

Siltala, Raimo, Johdatus oikeusteoriaan. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut, Helsinki 2001.

Siltala, Raimo, Oikeustieteen tieteenteoria. Suomalainen lakimiesyhdistys, Vammalan kirjapaino Oy, Vammala 2003.

Siltala, Raimo, Oikeudellisen ajattelun perusteet. Turun yliopiston oikeustieteellinen tiedekunta, Turku 2010.

Silvast, Antti, Making Electricity Resilient: Risk and Security in a Liberalized Infrastructure. Routledge 2017.

Talus, Kim – Penttinen, Sirja-Leena, Eurooppaoikeudelliset oikeuslähteet ja niiden tulkinta oikeustieteellistä opinnäytettä kirjoittaessa, s. 223–245. Teoksessa Miettinen, Tarmo (toim.), Oikeustieteellinen opinnäyte – Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodeista ja arvosteluista. Edita Publishing Oy 2016.

Wong, Helen, Cyber Security: Law and Guidance. Bloomsbury Professional Ltd 2018.

Virallislähteet

Energiavirasto, Energiaviraston ohje tietoturvallisuuteen liittyvän häiriön ilmoittamisesta (1914/402/2018).

Energiavirasto, Lausunto, Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti, 2781/403/2020, 04.01.2021.

Energiavirasto, Energiaviraston ohjeistus sähköverkonhaltijoiden varautumis- ja valmiussuunnittelusta 2022 (232/040002/2022).

Energiavirasto, Sähköverkonhaltijan varautumissuunnitelman mallipohja (232/040002/2022).

ENISA, ENISA Thread Landscape – Responding to the Evolving Thread Environment 2012.

Finanssivalvonta, Määräykset ja ohjeet 8/2014, Operatiivisen riskin hallinta rahoitussektorin valvottavissa, FIVA 8/01.00/2014.

HE 20/2013 vp. Hallituksen esitys eduskunnalle sähkö- ja maakaasumarkkinoita koskevaksi lainsäädännöksi.

HE 221/2013 vp. Hallituksen esitys eduskunnalle tietoyhteiskuntakaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta.

HE 39/2014 vp. Hallituksen esitys eduskunnalle laiksi luottolaitostoiminnasta ja eräiksi siihen liittyviksi laeiksi.

HE 50/2017 vp. Hallituksen esitys eduskunnalle maakaasumarkkinalaiksi ja eräiksi siihen liittyviksi laeiksi.

HE 192/2017 vp. Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta.

HE 212/2020 vp. Hallituksen esitys eduskunnalle laiksi sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä sekä eräiksi siihen liittyviksi laeiksi.

Huoltovarmuuskeskus (Axel Hagelstam), CIP – Kriittisen infrastruktuurin turvaaminen – Käsiteanalyysi ja kansainvälinen vertailu. Huoltovarmuuskeskus Julkaisuja 1/2005.

Huoltovarmuusorganisaation Digipooli, Kyberturvallisuuden nykytila eri toimialoilla – Kartoituksen keskeiset havainnot 2020.

Liikenne- ja viestintäministeriö, Verkko- ja tietoturvadirektiivi – Kansallista täytäntöönpanoa tukevan työryhmän loppuraportti. Liikenne- ja viestintäministeriön julkaisuja 9/2017.

Liikenne- ja viestintäministeriö, Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla – Työryhmän loppuraportti. Liikenne- ja viestintäministeriön julkaisuja 2021:1.

Liikenne- ja viestintävirasto, Määräys 67 teletoiminnan tietoturvasta, 67 A/2015 M.

Liikenne- ja viestintävirasto, Määräyksen 67 perustelut ja soveltaminen, MPS 67, 4.3.2015.

Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus, Kybersää huhtikuu 2022.

Liikenne- ja viestintävirasto, Määräyshankepäätös, Määräyksen 67 päivittäminen, 10.6.2022.

Oikeusministeriö, Viranomaisten toimivaltuudet häiriötilanteissa, Oikeusministeriön julkaisuja 2019:18.

Terveyden ja hyvinvoinnin laitos, Määräys 3/2021: Tietoturvasuunnitelmaan sisällytettävät selvitykset ja vaatimukset, THL/4309/4.09.00/2021, 20.12.2021.

Terveyden ja hyvinvoinnin laitos, Määräys 4/2021: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista, THL/4310/4.09.00/2021, 9.12.2021.

Terveyden ja hyvinvoinnin laitos, Määräys 5/2021: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista, THL/4311/4.09.00/2021, 9.12.2021.

Turvallisuuskomitea, Kyberturvallisuuden sanasto. Sanastokeskus TSK ry 2018.

Valtioneuvosto, Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017, 17.2.2017.

Valtioneuvosto, Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla. 10.6.2021.

Internetlähteet

Energiateollisuus ry 2022. Energiavuosi 2021 Sähkö. https://energia.fi/files/4428/Sahkovuosi_2021_netti.pdf (Luettu 19.5.2022).

Energiateollisuus ry 2022. Sähköntuotanto. https://energia.fi/energiasta/energiantuotanto/sahkontuotanto (Luettu 31.5.2022).

Energiateollisuus ry 2022. Sähköverkkojen rakenne. https://energia.fi/energiasta/energiaverkot/sahkoverkot (Luettu 19.5.2022).

Euroopan unionin neuvosto 2022. Lehdistötiedote: Vahvempi kyberturvallisuus ja häiriönsietokyky koko EU:hun – neuvoston ja Euroopan parlamentin alustava yhteisymmärrys. https://www.consilium.europa.eu/fi/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/ (Luettu 20.7.2022).

Fingrid Oyj 2022. Fingridin sähkönsiirtoverkko. https://www.fingrid.fi/kantaverkko/sahkonsiirto/fingridin-sahkonsiirtoverkko/ (Luettu 19.5.2022).

Fingrid Oyj 2022. Suomen sähköjärjestelmä. https://www.fingrid.fi/kantaverkko/sahkonsiirto/suomen-sahkojarjestelma/ (Luettu 19.5.2022).

Liikenne- ja viestintävirasto 2022. Sääntelyn kohteet. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/saantelyn-kohteet. (Luettu 28.11.2022).

Oikeusministeriö 2022. Lainkirjoittajan opas. 13.10 Kielto valtuuttaa “ohjeiden antamiseen. http://lainkirjoittaja.finlex.fi/13-saadosten-lajit-ja-saadostaso/13-10/ (Luettu 2.1.2023).

USSOCOM. https://media.defense.gov/2022/Apr/28/2002985725/-1/-1/1/SOCOM_22D_R1.PDF (Luettu 16.6.2022).

Lyhenteet

APT – Advanced Persistent Threat

CSIRT-toimija – Computer Security Incident Response Team

ICS-järjestelmä – Industrial Control System

ICT-järjestelmä – Information and Communications Technology

NIS-direktiivi – EU:n verkko ja tietoturvadirektiivi (Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa)

NIS2 -direktiivi – EU:n kyberturvallisuusdirektiivi (Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta)

SCADA-järjestelmä – Supervisory Control And Data Acquisition

SVPL – Laki sähköisen viestinnän palveluista (917/2014)

SWOT-analyysi – Strenghts, Weaknesses, Opportunities, Threats

1 Johdanto

1.1 Tutkielman aihe ja tutkimuskysymykset

Tutkielman tarkoituksena on kartoittaa sähköverkonhaltijoita velvoittavaa kyberturvallisuussääntelyä, arvioida sen toimivuutta ja esittää siihen parannuksia.

Energiahuolto, jonka merkittävänä osana sähköverkot toimivat, on määritelty joka puolella maailmaa yhdeksi tärkeimmistä kriittisen infrastruktuurin osa-alueista.[1] Kuten muutkin kriittiset toimijat tänä päivänä, myös sähköverkonhaltijat ovat hyvin pitkälti riippuvaisia toimivista ja turvallisista tietojärjestelmistä sekä tietoverkoista.[2] Tästä syystä näihin kohdistuvat kyberturvallisuusvaatimukset ovat merkittävä osa sähköverkkojen toimintavarmuutta, ja sitä kautta koko yhteiskunnan toimintaa ja turvallisuutta.

Tutkielman tutkimuskysymykset ovat seuraavat:

1. Miten sähköverkkojen kyberturvallisuutta säännellään?

2. Miten muiden kriittisten toimialojen kyberturvallisuutta säännellään?

3. Miten sähköverkonhaltijoihin kohdistuvaa kyberturvallisuussääntelyä tulisi kehittää, jotta kyberuhkiin pystyttäisiin varautumaan paremmin?

Varsinaista oikeustieteellistä tutkimusta pohjustetaan ensin luvussa 2, jossa esitellään sähköverkkoinfrastruktuuria ja selvitetään sähköverkonhaltijoihin kohdistuvia kyberuhkia. Tämän jälkeen tutkielman pääluvut seuraavat tutkimuskysymyksiä niin, että luvussa 3 vastataan ensimmäiseen tutkimuskysymykseen, luvussa 4 toiseen kysymykseen ja luvussa 5 kolmanteen.

1.2 Tutkimusmetodit

Tutkielman tutkimusmetodeina ovat *lainopillinen tutkimus* sekä *de lege ferenda* -tyylinen pohdinta. Lainopillinen tutkimus keskittyy sähköverkkojen kyberturvallisuussääntelyn kartoittamiseen, jäsentämiseen ja tulkintaan. Tutkielmassa selvitetään keskeisimmät säännökset aina EU-tasolta kansalliseen lainsäädäntöön ja lakia alemman asteiseen sääntelyyn

[1] Huoltovarmuuskeskus 2005, s. 22.

[2] Liikenne- ja viestintäministeriö 2021, s. 17.

asti. Lainopillisessa analyysissä pohditaan näiden säännösten sisältöä, keskinäisiä suhteita, ja selvitetään sähköverkonhaltijoihin kohdistuvat kyberturvallisuusvelvoitteet.

Velvoitesäännösten lisäksi tutkimus kohdistuu toimivaltaisia viranomaisia ja kyberturvallisuusvelvoitteiden valvontaa koskevaan sääntelyyn, sekä velvoitteiden noudattamatta jättämisestä seuraavaan sanktiosääntelyyn. Analyysin pohjalta muodostetaan kokonaiskuva tämänhetkisestä oikeustilasta.

Lainopillisessa tutkimuksessa kartoitetaan myös valikoivasti muiden kriittisten toimialojen kyberturvallisuussääntelyä. Vertailemalla eri alojen sääntelyä keskenään, voidaan saada arvokasta tietoa eri alojen parhaista käytänteistä.

Sen jälkeen kun vallitsevasta oikeustilasta on saatu mahdollisimman tarkka kuva lainopillisen analyysin avulla, tutkielmassa pohditaan de lege ferenda -hengessä sitä, miten sähköverkkojen kyberturvallisuussääntelyä tulisi tulevaisuudessa kehittää.

1.3 Tutkielman tausta ja yhteiskunnallinen merkitys

Tutkielma on saanut innoituksensa *Valtioneuvoston periaatepäätöksestä tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla*,[3] sekä erityisesti periaatepäätöstä edeltäneestä *liikenne- ja viestintäministeriön raportista*[4]. Raportista käy ilmi, että tällä hetkellä eri kriittisiin toimialoihin kohdistuu lainsäädännössä keskenään hyvin erilaisia kyberturvallisuusvelvoitteita.[5] Toiset alat ovat kattavammin säänneltyjä kuin toiset; kyberturvallisuussääntelyn osalta paras tilanne on tällä hetkellä rahoitus- ja televiestintä-aloilla. Sen sijaan esimerkiksi energiahuollon, liikenteen ja vesihuollon sektoreilla tilanne on huonompi, sillä näillä toimialoilla laintasoinen sääntely ei ole yhtä kattavaa.[6]

Tutkimuksen kohteena olevaksi toimialaksi on valittu sähköverkot, sillä energiahuollon merkittävänä osana ne vaikuttavat käytännössä kaikkien muiden kriittisten toimialojen

---

[3] Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla. 21.7.2021.

[4] Liikenne- ja viestintäministeriö, Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla – Työryhmän loppuraportti. Liikenne- ja viestintäministeriön julkaisuja 2021:1.

[5] Liikenne- ja viestintäministeriö 2021, s. 28.

[6] Liikenne- ja viestintäministeriö 2021, s.29.

toimintaan.[7] Oli sitten kyse vesihuollon järjestämisestä, ruoantuotannosta, kriittisestä tehdastuotannosta tai finanssimarkkinoiden toiminnasta, kaikkialla tarvitaan sähköä. Nyky-yhteiskunta ei yksinkertaisesti enää kykene toimimaan, mikäli sähkönsaanti katkeaa.

Myös kansalliseen turvallisuuteen kohdistuvat uhat ovat jo pidemmän aikaa olleet aiempaa monimuotoisempia. Siinä missä joitakin vuosikymmeniä sitten turvallisuuskeskustelussa puhuttiin lähinnä *sotilaallisesta vaikuttamisesta*, nykyinen uhkakenttä on monipuolistunut ja keskusteluun on noussut uusia termejä, kuten *hybridivaikuttaminen*.[8] Yhteiskunnan turvallisuuden kannalta kriittisiin toimijoihin kohdistuvat uhat kasvattavat jatkuvasti merkitystään.[9] Poikkeusoloihin varautumisen lisäksi, *normaaliolojen häiriötilanteisiin* varautuminen on siis nykyisin vähintäänkin yhtä tärkeää.

Kuten jo edellä tuotiin esille, yhteiskunnan turvallisuuden kannalta kriittiset toimijat, mukaan lukien sähköverkonhaltijat, nojaavat käytännön toiminnassaan pitkälti digitaalisiin tietojärjestelmiin ja -verkkoihin. Näihin kohdistuvat kyberuhat eivät ole pelkästään teoriaa, vaan täyttä totta. Pahantahtoista kybertoimintaa voi kohdistua niin yksittäisiin yrityksiin kuin valtion instituutioihinkin. Kyberhyökkäyksen tekijänä voivat olla yksityiset rikolliset toimijat, vieraat valtiot tai näiden käyttämät bulvaanit.[10]

Tunkeutumalla esimerkiksi sähköverkkoja hallinnoiviin tietojärjestelmiin, hyökkääjä voi häiritä sähköverkon toimintaa tai pahimmassa tapauksessa katkaista sähkönjakelun kokonaan. Näin tapahtui esimerkiksi Ukrainassa joulukuussa 2015, kun sähköverkkoja hallinnoivat järjestelmät saastuttanut haittaohjelma BlackEnergy katkaisi sähköt laajoilta alueilta. Yhdysvaltain viranomaisten tutkimusten perusteella BlackEnergy haittaohjelma näyttäisi olevan lähtöisin Venäjältä.[11]

Venäjän helmikuussa 2022 aloittama hyökkäyssota Ukrainassa on jälleen kerran muuttanut koko Euroopan turvallisuustilannetta. Myös Suomi on entistä huolestuneempi turvallisuutensa puolesta. Suomen tuore NATO-hakemus on varmasti omiaan lisäämään jo aiemminkin

---

[7] Pöyhönen 2020, s. 112.
[8] Aine – Nurmi – Valtonen 2022, s. 841.

[9] Aine – Nurmi – Ossa – Penttilä – Salmi – Virtanen 2011, s. 3–36.

[10] Liikenne- ja viestintäministeriö 2021, s. 40.

[11] Perez CNN, 4.2.2016.

yleistynyttä Venäjän harjoittamaa hybridivaikuttamista, jonka osana myös erilaisten kyberhyökkäysten riski kasvaa. Sodan alkamisen jälkeen olemme jo joutuneet todistamaan merkittäviä hyökkäyksiä kriittistä infrastruktuuria vastaan, mistä esimerkkinä Nord Stream -kaasuputkien räjäyttäminen syyskuussa 2022. Länsi epäilee sabotaasista Venäjää.[12]

Kyberturvallisuuskeskuksen kuukausittain julkaiseman *Kybersään* mukaan myös teollisuusautomaatiojärjestelmiin ja yleisemmin kriittisiin toimijoihin kohdistuvat kyberuhat ovat lisääntyneet kiristyneen geopoliittisen tilanteen myötä.[13] Teollisuusautomaation kyberuhkia käsitellään laajemmin luvussa 2.2.3. Samassa kybersään julkaisussa viitataan myös yhdysvaltalaiseen raporttiin[14], jonka mukaan eri maiden asevoimat panostavat parhaillaan voimakkaasti kriittiseen infrastruktuuriin suunnattujen kyberaseiden kehittämiseen. Kriittisten toimialojen kyberturvallisuuden ja kriisinkestävyyden tutkiminen on siis ajankohtaisempaa kuin koskaan.

1.4 Tutkielman rajaus ja rakenne

Oikeustieteen maisterin opinnäytetyön ohjeellisen laajuuden vuoksi, tutkimus keskittyy suurimmaksi osaksi vain yhteen kriittiseen toimialaan, eli sähköverkkoihin. Sähköverkkojen painoarvoa merkittävänä toimialana on käsitelty edellisissä luvuissa. Toimiala on mielenkiintoinen myös siitä syystä, että kuten tutkielmassa tullaan esittämään, alan velvoittavassa kyberturvallisuussääntelyssä vaikuttaisi olevan kehitettävää. Sähköverkkojen osalta tarkastellaan tarkemmin ottaen *sähköverkonhaltijoita* ja niitä velvoittavaa sääntelyä. Käsitettä avataan tarkemmin luvussa 2.1.

Lainopillinen analyysi on rajattu koskemaan kyberturvallisuussääntelyn ydinaluetta, eli varsinaista *velvoitesääntelyä*, *viranomaisvalvontaa koskevaa sääntelyä* sekä velvoitteisiin liittyvää *sanktiosääntelyä*. Aihetta voitaisiin lähestyä myös monista muista näkökulmista, kuten perusoikeudellisesta tai sopimusoikeudellisesta näkökulmasta. Mielenkiintoinen vaihtoehtoinen tarkastelutapa tutkimuksen tematiikkaan voisi siten olla esimerkiksi sähköverkkoyhtiöiden perustuslain mukaiset oikeudet liiketoimintansa vapaaseen harjoittamiseen suhteessa resursseja vaativiin kyberturvallisuustoimiin, tai esimerkiksi

---

[12] Mykkänen HS, 18.11.2022.

[13] Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus 2022.

[14] USSOCOM (https://media.defense.gov/2022/Apr/28/2002985725/-1/-1/1/SOCOM_22D_R1.PDF).

velvoitteiden tarkasteleminen toimijoiden välisten sopimusten osana. Viimeiseksi mainitussa tutkimusnäkökulmassa voitaisiin esimerkiksi tarkastella tilannetta, jossa kriittisen toimialan yritys on ulkoistanut osan kyberturvallisuustoimistaan ulkopuoliselle tietoturvayhtiöllä. Tällaisessa tilanteessa olisi tärkeää, että toimijoiden välinen vastuunjako olisi määritelty sopimuksissa mahdollisimman tarkasti.[15] Tilanteeseen liittyvässä tutkimuksessa voitaisiin arvioida esimerkiksi sitä, kummalla sopimusosapuolella olisi loppupeleissä vastuu turvallisuudesta huolehtimisesta ja kuka joutuisi korvausvastuuseen kyberhyökkäyksistä aiheutuneista vahingoista.

Tässä tutkimuksessa keskitytään nimenomaan kyberympäristöön ja sen kautta tapahtuviin hyökkäyksiin. Toisin sanoen fyysisen maailman hyökkäykset, kuten esimerkiksi sähköverkkojen eri osien suora sabotoiminen eivät tule tässä tutkielmassa tarkasteltaviksi. Kyberturvallisuus on käsitteenä laaja ja se pitää sisällään erilaisia osa-alueita, joita avataan tarkemmin tutkimusta pohjustavassa luvussa 2.2.1.

Tutkimus liikkuu vahvasti normaaliolojen häiriötilanteiden alueella, ja tarkemmin ottaen kyberturvallisuussääntelyä on tarkoitus tarkastella nimenomaan *varautumisen* näkökulmasta. Tutkimus ei siis painotu koskemaan tilanteita, joissa kyberhyökkäys *on jo tapahtunut*, vaikka tällaistakin tilannetta käsittelyssä sivutaan. Tutkimuksessa ei myöskään nimenomaisesti käsitellä kyberrikollisuutta tai lähestytä aihetta rikosoikeudellisesta näkökulmasta.

Kriittisten toimijoiden kyberturvallisuusvelvoitteisiin liittyvää oikeuskäytäntöä ei joko ole, tai se on joka tapauksessa hyvin vähäistä.[16] Ainakaan tätä tutkimusta tehtäessä, relevanttia oikeuskäytäntöä ei ole tullut missään vaiheessa vastaan, mikä on itsessään mielenkiintoinen ja kysymyksiä herättävä huomio. Oikeuskäytännön puute voi kieliä esimerkiksi siitä, että kriittisiin toimijoihin kohdistuneet kyberhyökkäykset eivät ole syystä tai toisesta johtaneet oikeusprosesseihin. Voi olla, että kyberturvallisuustoimien laiminlyömisestä eri tahoille aiheutuneet vahingot on kyetty kompensoimaan esimerkiksi sovittelemalla. Toisaalta voi myös olla, että kyberturvallisuusvelvoitteisiin liittyvä sääntely on nykyisellään siinä määrin epätäsmällistä, ettei kriittisiä toimijoita vastaan ole pystytty edes aloittamaa oikeusprosesseja tilanteissa, joissa ne ovat laiminlyöneet velvoitteensa. Joka tapauksessa, kyberturvallisuuden

[15] Lonka – Limnéll 2015, s. 204.

[16] Lahti 2022, s. 13.

häiriötilanteista mahdollisesti seuraavat riita- ja rikosprosessit on ollut pakko jättää tässä tutkielmassa tarkastelun ulkopuolelle.

Tutkielman alussa, luvussa 2 pohjustetaan varsinaista lainopillista analyysiä, esittelemällä sähköverkkojen infrastruktuuria, toimintaa sekä tietojärjestelmiä ja -verkkoja niiden merkittävänä osana. Lisäksi luvussa käsitellään kyberturvallisuutta yleisellä tasolla ja esitellään sähköverkkoja hallinnoiviin tietojärjestelmiin kohdistuvia merkittävimpiä kyberuhkia.

Luvussa 3 syvennytään tutkielman pääaiheeseen, eli sähköverkkojen kyberturvallisuussääntelyn lainopilliseen analyysiin. Ensimmäisenä käsitellään kyberturvallisuuden velvoitesääntelyä ja tämän jälkeen velvoitteiden noudattamiseen liittyvää viranomais-, valvonta- ja sanktiosääntelyä. Kunkin sääntelymuodon osalta käsitellään eri tasoista ja eri tavalla velvoittavaa sääntelyä EU-tasolta aina lakia alemman asteiseen sääntelyyn asti.

Luvussa 4 esitellään valikoivasti muiden kriittisten toimialojen kyberturvallisuussääntelyä ja vertaillaan tätä sähköverkkojen sääntelyyn.

Luvussa 5 esitetään aiempien lukujen tutkimuksen, kirjallisuuden ja viranomaislähteiden perusteella parannusehdotuksia nykyiseen sähköverkkojen kyberturvallisuussääntelyyn. Viimeisessä luvussa 6 vedetään yhteen koko tutkielman johtopäätökset, heränneet ajatukset ja esitetään aiheita mahdolliselle jatkotutkimukselle.

2 Sähköverkot ja niiden kyberturvallisuus

2.1 Sähköverkkojen infrastruktuuri ja toiminta

Ennen kuin päästään käsittelemään varsinaisesti sähköverkkojen kyberturvallisuutta ja siihen liittyvää lainsäädäntöä, on hyvä hieman pohjustaa itse toimintakenttää. Tässä luvussa annetaan kokonaiskuva Suomen sähköverkkojen infrastruktuurista, alan toimijoista sekä sähkömarkkinoista. Sähkömarkkinoilla toimii lukuisia yrityksiä erilaisissa rooleissa, ja luvun tarkoituksena onkin lisäksi edelleen rajata tutkimuskohdetta *sähköverkonhaltijan* käsitteen avulla.

Suomen sähköjärjestelmä koostuu voimalaitoksista, kantaverkosta, suurjännitteisistä jakeluverkoista, jakeluverkoista sekä sähkön kuluttajista. Se on osa yhteispohjoismaista sähköjärjestelmää yhdessä Ruotsin, Norjan ja Itä-Tanskan järjestelmien kanssa. Lisäksi Venäjältä ja Virosta on Suomeen tasasähköyhteydet, joilla pohjoismainen järjestelmä on yhdistetty Venäjän ja Baltian voimajärjestelmään.[17]

Sähkön tuotanto alkaa *voimalaitoksista*, joita on Suomessa noin 400. Suomalainen sähköntuotanto on kansainvälisesti vertailtuna hyvin hajautettua, eli sähköä tuotetaan monilla eri tavoilla. Tämä on hyväksi energian huoltovarmuudelle, sillä Suomi on näin ollen vähemmän riippuvainen tietyn tuotantotavan toiminnasta tai raaka-aineiden saatavuudesta.[18] Sähköntuotannossa ollaan myös menossa vahvasti kohti fossiilivapaita energianlähteitä, ja meillä tuotetaan jo nyt iso osa sähköstä ydinvoimalla ja vesivoimalla. Sähkön yhteistuotanto kaukolämpövoimaloissa sekä teollisuuden yhteydessä on myös merkittävä osa tuotantoa.[19]

Suomi joutuu vielä toistaiseksi tuomaan osan sähköstä ulkomailta, esimerkiksi muista Pohjoismaista, mutta sähköomavaraisuutta ollaan koko ajan kehittämässä. Kantaverkkoyhtiö Fingridin mukaan Suomesta on tulossa vuositasolla sähköomavarainen jo lähitulevaisuudessa. Iso syy omavaraisuuden kasvuun ovat muun muassa merkittävät investoinnit tuulivoimaan.[20]

---

[17] Fingrid Oyj 2022.

[18] Energiateollisuus ry 2022.

[19] Energiateollisuus ry 2022.

[20] Hämäläinen TM 2021, s. 67.

Kantaverkko muodostaa Suomen sähkönsiirtojärjestelmän selkärangan ja kantaverkonhaltijana toimii Fingrid Oyj. Kantaverkko muodostuu korkeajännitteisistä voimalinjoista, jotka kulkevat läpi Suomen ja vastaavat sähkönsiirrosta pitkillä välimatkoilla. Kantaverkon kautta kulkee noin 77 prosenttia Suomessa siirretystä sähköstä.[21]

Voimalaitokset sekä suuret tehtaat ovat usein kytkeytyneet suoraan kantaverkkoon. Muille sähkön loppukäyttäjille, kuten pienemmälle teollisuudelle, kaupalle ja kuluttajille, sähkö kulkee kantaverkkoon liitettyjen *jakeluverkkojen* kautta. Jakeluverkot voivat olla pidemmillä siirtomatkoilla suurjännitteisiä, kun taas paikallisesti käytetään niin sanottuja tavallisia jakeluverkkoja, joiden nimellisjännite on alle 110 kilovolttia.[22] Jakeluverkoista vastaavat jakeluverkonhaltijoina toimivat yritykset, kuten esimerkiksi Caruna Oy tai Turku Energia Sähköverkot Oy.

Konkreettisesti sähköverkot koostuvat joko ilmassa tai maan alla kulkevista sähköjohdoista, sekä erilaisista sähköasemista ja jakelumuuntamoista. Asemilla ja muuntamoissa eri jännitetasoilla toimivat sähköverkot yhdistyvät toisiinsa ja niiden kautta sähkön jakelua eri verkon osille voidaan säädellä.[23]

Sähkömarkkinalain (588/2013) 3 §:n yhdeksännen kohdan mukaan *verkonhaltijalla* tarkoitetaan elinkeinonharjoittajaa, jolla on hallinnassaan sähköverkkoa ja joka harjoittaa luvanvaraista sähköverkkotoimintaa tässä verkossa. Käytännössä verkonhaltijalla viitataan joko kantaverkonhaltijaan tai jakeluverkonhaltijoihin. Verkonhaltijat, jotka siis vastaavat sähkön siirtämisestä voimalaitoksista loppukäyttäjille, ovat merkittävässä osassa sähköjärjestelmää ja siten koko kriittisen infrastruktuurin toimintaa. Tässä tutkimuksessa keskitytään nimenomaan verkonhaltijoihin ja niiden käyttämien tietojärjestelmien kyberturvallisuuteen. Tekstissä käytetään termejä verkonhaltija ja sähköverkonhaltija synonyymeinä.

Sähkömarkkinat termillä viitataan nykyään yleisimmin Pohjoismaiden yhteisiin sähkömarkkinoihin, joilla kauppa alkaa siitä, kun *sähköntuottajat* tarjoavat sähköä myytäväksi sähköpörssiin. Sähkön *vähittäismyyjinä* toimivat yritykset puolestaan ostavat ja

---

[21] Fingrid Oyj 2022.

[22] Energiateollisuus ry 2022.

[23] Energiateollisuus ry 2022.

jälleenmyyvät tätä sähköä kuluttajille, ja konkreettisesti sähkö siirretään loppukäyttäjille *verkonhaltijoiden* hallinnoimien sähköverkkojen välityksellä. Pohjoismaiden yhteisenä sähköpörssinä toimii *Nord Pool*, jossa käydään kauppaa päivittäin ja jopa tunnin aikajaksoilla. Järjestelmän tarkoituksena on taata sähköntuotannon ja -välityksen tehokkuus, alhaiset kustannukset ja riittävä sähkönsaanti kaikkialla Pohjoismaissa.[24] Ajatuksena on, että sähköä tuotetaan Pohjoismaissa siellä, missä tuotanto on kullakin hetkellä halvinta ja tehokkainta, minkä jälkeen tuotettu sähkö myydään ja siirretään eteenpäin sinne, missä sitä tarvitaan. Esimerkiksi sateisina vuosina keskimääräistä suurempi osa sähköstä tuotetaan vesivoimalla, jolloin Suomeen tuodaan tavallista enemmän sähköä Norjan suurista vesivoimaloista.

Toimivat sähkömarkkinat ja onnistunut kauppa sähköpörssissä ovat toki merkittävä osa sähkön toimitusvarmuutta, mutta tässä tutkielmassa asiaan ei perehdytä tämän syvällisemmin.

2.2 Sähköverkonhaltijoiden tietojärjestelmät ja niiden kyberturvallisuus

2.2.1 Kyberturvallisuus yleisesti

Kyberturvallisuus on laaja käsite, jolle voidaan antaa asiayhteydestä riippuen hieman erilaisia määritelmiä. Yhteistä kaikille määritelmille on kuitenkin se, että kyberturvallisuus liittyy aina digitaalisiin järjestelmiin ja yleisesti digitalisoituneeseen yhteiskuntaan. Erään määritelmän mukaan kyberturvallisuus on kokonaisturvallisuuden osa-alue, jolla pyritään digitalisoituneen ja verkottuneen yhteiskunnan turvallisuuteen. Kyberturvallisuudessa yhdistyvät tietoturva, toimintojen jatkuvuuden hallinta ja häiriötilanteisiin varautuminen. Organisaatioiden kyberturvallisuus muodostuu kyvykkyyksistä, kuten ihmisten osaamisesta ja käytänteistä, sekä prosesseista ja teknologioista, joilla voidaan suojata verkkoja, järjestelmiä, laitteita ja dataa hyökkäyksiltä tai luvattomalta käytöltä.[25]

Kyberturvallisuus on siis kaikkia niitä valmiuksia ja toimia, joilla organisaatio pystyy varmistamaan tietojärjestelmiensä ja -verkkojensa turvallisuuden sekä moitteettoman toiminnan. Käytännössä tämä tarkoittaa esimerkiksi sitä, että organisaation käyttämät järjestelmät ovat teknisiltä ratkaisuiltaan turvallisia, niitä suojataan ja valvotaan tehokkaasti ja organisaatiossa olevat ihmiset tuntevat turvalliset toimintatavat sekä myös noudattavat niitä.

---

[24] Silvast 2017, s. 77–80.

[25] Pöyhönen 2020, s. 32.

Organisaation päivittäisessä arjessa kyberturvallisuus näkyy luonnollisesti teknisten järjestelmien toimivuudesta ja turvallisuudesta vastaavien henkilöiden työssä, mutta myös esimerkiksi siinä, millaisia pääsynhallinta ja salasanakäytänteitä muutkin organisaation työntekijät noudattavat. Ainakin isommille yrityksille on myös tyypillistä, että organisaation kyberturvallisuus on osittain ulkoistettu tähän erikoistuneelle alan yritykselle, joka käyttää tarvittaessa omia ohjelmistojaan organisaation suojaamiseen ja valvontaan.[26]

Tietoturva on käsitteenä hieman suppeampi kuin kyberturvallisuus. Siinä missä kyberturvallisuus koskee yleisesti koko digitalisoitunutta yhteiskuntaa, tietoturva taas liittyy nimenomaan tiedon turvaamiseen. Koska suurin osa tiedosta on tänä päivänä digitaalisissa järjestelmissä, käytetään termejä kuitenkin usein käytännössä samassa asiayhteydessä. Turvallisuuskomitean julkaisema *Kyberturvallisuuden sanasto* määrittelee tietoturvan tai tietoturvallisuuden järjestelyiksi, joilla pyritään varmistamaan tiedon *saatavuus*, *eheys* ja *luottamuksellisuus*. Saatavuus tarkoittaa sitä, että tieto on hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa. Tietoturvan järjestelyjä ovat esimerkiksi kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelmien ja varmenteiden käyttö.[27] Johdonmukaisuuden vuoksi tässä tutkielmassa pitäydytään enimmäkseen termissä kyberturvallisuus, vaikka tietyissä yhteyksissä voitaisiin yhtä hyvin käyttää termiä tietoturva.

2.2.2 Kyberuhat

Digitalisaatio on tehostanut organisaatioiden ja yksityishenkilöiden toimintaa kaikilla yhteiskunnan aloilla, mutta sen kääntöpuolena ovat tulleet kyberuhat. Vaikka organisaatiossa olisi käytössä viimeisin teknologia ja kyberturvallisuudesta huolehdittaisiin muutenkin parhaalla mahdollisella tavalla, mikään organisaatio tai järjestelmä ei ole täydellinen ja sisältää aina haavoittuvuuksia, joita vihamielinen toimija voi pyrkiä hyödyntämään.

Käytännössä kyberhyökkäys voidaan toteuttaa monella eri tavalla. Valtioneuvoston vuonna 2017 julkaisemassa tutkimusraportissa *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi* kuvataan viime vuosien

[26] Pöyhönen 2020, s. 171.

[27] Turvallisuuskomitea 2018, s. 15.

kyberhyökkäysten megatrendejä. Esimerkkeinä mainitaan muun muassa kiristyshaittaohjelmat, haavoittuvuuksien hyödyntäminen, laitteistoihin kohdistuvat uhat, yrityksen sisäpiiri hyökkäyskanavana, huijaukset, tietojen kalastelu, palvelunestohyökkäykset sekä kohdistetut hyökkäykset.[28]

Haavoittuvuuksien hyödyntäminen nähdään yhtenä merkittävimmistä keinoista tunkeutua organisaatioiden tietojärjestelmiin. Kyberrikolliset luovat koko ajan kehittyneempiä ja teknisesti edistyksellisempiä keinoja, joilla voidaan päästää käsiksi yhä syvemmälle kohdeorganisaation järjestelmiin ja toimia siellä entistä huomaamattomammin.[29]

Haavoittuvuudet voivat olla *teknisiä* tai ne voivat liittyä *ihmisten toimintaan*. Esimerkki järjestelmän teknisestä haavoittuvuudesta on tilanne, jossa hyökkääjä pääsee organisaation tietojärjestelmään sisälle suoraan verkon välityksellä, hyödyntämällä järjestelmässä olevaa *tietoturva-aukkoa*. Esimerkki ihmisten toiminnasta aiheutuvasta haavoittuvuudesta on puolestaan tilanne, jossa hyökkääjä onnistuu kalastelemaan organisaation työntekijöiden käyttäjätunnuksia ja salasanoja, ja pääsee näiden avulla kirjautumaan sisälle järjestelmiin, tai tilanne, jossa hyökkääjä ujuttaa organisaation tietojärjestelmään haittaohjelman henkilökunnalle lähetettävän sähköpostin liitteenä.[30]

2.2.3 Sähköverkonhaltijoiden tietojärjestelmät ja niihin kohdistuvat kyberuhat

Nykyään sähköverkkoja hallinnoidaan kehittyneiden ja monimutkaisten digitaalisten tietojärjestelmien ja -verkkojen avulla. Jouni Pöyhönen kuvaa väitöstutkimuksessaan *Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa – Systeemiajattelu* sähköyhtiölle tyypillistä tietojärjestelmien infrastruktuuria. Järjestelmät voidaan jakaa karkeasti kahdelle tasolle, jotka ovat *yritystaso* ja *tuotantotaso*.[31]

Yritystasolla puhutaan ICT-järjestelmistä (Information and Communication Technology), joilla hallinnoidaan yrityksen toimintaa organisaation korkeimmalla tasolla, aina yrityksen

---

[28] Valtioneuvosto 2017, s. 12.

[29] Valtioneuvosto 2017, s. 12.

[30] Pöyhönen 2020, s. 114 (Lehto, M., 2015, Phenomena in the Cyber World. Cyber Security: Analytics, Technology and Automation. Springer 2015, pages 3-29.).

[31] Pöyhönen 2020, s. 108.

strategisesta johtamisesta henkilöstöhallintoon. Konkreettisesti nämä ICT-järjestelmät muodostuvat palvelimista, tietojärjestelmistä ja tietoverkoista, jotka toimivat joko kiinteän tai langattoman verkon välityksellä, joko organisaation sisäisesti tai yhteydessä julkiseen internetiin.[32] Käytännössä tarkoitetaan siis normaaleja tietokoneita ja järjestelmiä, jollaisia on nykypäivänä käytössä kaikissa toimistoympäristöissä.

Tuotantotasolla puolestaan puhutaan usein *teollisuusautomaatiosta*, joka tarkoittaa tietojärjestelmien hyödyntämistä fyysisten koneiden ja tuotantoprosessien ohjaamisessa. Tässä yhteydessä voidaan puhua myös automaatiojärjestelmistä, eli ICS-järjestelmistä (Industrial Control System). Automaatiojärjestelmillä ohjataan suoraan jonkin fyysisen laitteen toimintaa ja ne on usein suunniteltu ja koodattu nimenomaan kyseistä toimintoa varten.[33] Järjestelmät ovat myös tyypillisesti pitkäikäisiä ja niitä päivitetään harvoin. Automaatiojärjestelmät voivat olla monella tavalla yhteydessä niin yritystason järjestelmiin, kuin myös muuhun maailmaan, joko organisaation sisäisen verkon tai julkisen internetin välityksellä.[34]

Sähköverkonhaltijat hyödyntävät teollisuusautomaatiota hallitessaan sähkönjakelua sähköverkon eri osille. Käytännössä tämä tarkoittaa esimerkiksi sitä, että verkonhaltijayrityksen valvomossa työskentelevä työntekijä säätää etäohjauksella jonkin sähköaseman kytkimiä ja vaikuttaa tätä kautta sähkön kulkuun sähköverkossa.[35] Etäohjaukseen käytetään usein SCADA-järjestelmää (Supervisory Control And Data Acquisition), jonka heikkouksia on käsitelty paljon kriittisen infrastruktuurin kyberturvallisuutta käsittelevässä kirjallisuudessa. Järjestelmää ei pidetä erityisen tietoturvallisena, sillä se perustuu vanhaan teknologiaan, eikä sitä ole alun perin suunniteltu yhdistettäväksi julkiseen verkkoon.[36]

---

[32] Pöyhönen 2020, s. 108–109.

[33] Bayuk ym., s. 58–59.

[34] Pöyhönen 2020, s. 109–112.

[35] Silvast 2017, s. 117.

[36] Wong 2018, s. 116.

Mikäli jokin vihamielinen taho haluaisi vaikuttaa sähköverkon toimintaan, se voisi aloittaa kyberhyökkäyksen esimerkiksi ujuttamalla haittaohjelman verkonhaltijan tietojärjestelmiin.[37] Sisään järjestelmiin voidaan päästä montaakin eri kautta, esimerkiksi hyödyntämällä edellä mainitulla tavalla organisaation henkilöstöä tai järjestelmien tietoturva-aukkoja. Koska tietojärjestelmät ja niiden eri osat organisaatioissa ovat tänä päivänä niin vahvasti verkottuneita, voi yhteen osaan tunkeutuminen johtaa niin sanottuun *kaskadi-ilmiöön*, jossa häiriö voi päästä leviämään laajalle ja vaikuttamaan useampiin eri alijärjestelmiin.[38]

Tuli verkonhaltijayritykseen kohdistunut hyökkäys sitten mitä kautta tahansa, sen lopullisena tavoitteena on tyypillisesti pyrkiä vaikuttamaan juuri automaatiojärjestelmän toimintaan. Esimerkiksi vuonna 2015 Ukrainan sähköverkkoon tehty hyökkäys toteutettiin teollisuusautomaatiojärjestelmään kohdistetulla hyökkäyksellä. Hyökkäyksen myötä sähköasemien etäkäyttö onnistuttiin poistamaan väliaikaisesti käytöstä, jolloin sähköaseman sääteleminen ei enää onnistunut verkonhaltijayrityksen valvomosta. Hyökkääjä onnistui ottamaan haltuun kyseisen automaatiojärjestelmän ja katkaisemaan sähköt 230 000 ihmiseltä.[39] Tapauksessa yhtiön automaatiojärjestelmät saastuttanut haittaohjelma onnistuttiin alun perin ujuttamaan sisään yhtiön työntekijälle lähetetyn sähköpostiviestin liitteenä.[40]

Sähköverkkoyhtiön yritystason ICT-järjestelmät ja tuotantotason ICS-järjestelmät muodostavat siis monimutkaisen digitaalisen kokonaisuuden, jonka suojaustoimenpiteet edellyttävät kyberuhkien laaja-alaista analysointia ja riskiarvioiden tekemistä. Suojausratkaisuja suunniteltaessa huomiota joudutaan kohdistamaan molempiin tasoihin, sekä niiden keskinäiseen vuorovaikutukseen.[41] Kriittisen infrastruktuurin organisaatioilla on onneksi mahdollisuus suojata järjestelmiään kyberhyökkäyksiltä monenlaisilla teknisillä ratkaisuilla ja organisaatiossa omaksutuilla käytänteillä.[42]

---

[37] Pöyhönen 2020, s. 114.

[38] ENISA 2012, s. 32.

[39] Carter 2017.

[40] Hyppönen 2021, s. 247

[41] Pöyhönen 2020, s. 114.

[42] Wong 2018, s. 151–152.

Kiristyneen geopoliittisen tilanteen vuoksi, teollisuusautomaatiojärjestelmät vaikuttavat olevan entistä suoraviivaisempien kyberhyökkäysten kohteena. Aiemmin kriittistä infrastruktuuria vastaan tehdyt hyökkäykset ovat alkaneet tyypillisesti yritystason perustietotekniikkaan (ICT) kohdistetulla hyökkäyksellä, jonka välityksellä on sitten pyritty vaikuttamaan teollisuusautomaation toimintaan. Tämä toimintatapa on ollut rikollisille usein tuottavampi vaihtoehto, sillä ICT järjestelmiin on ollut helpompi tunkeutua, kuin hyvin yksilöllisesti suunniteltuihin teollisuusautomaatiojärjestelmiin. Tilanteessa on kuitenkin nähtävissä muutosta, ja esimerkiksi valtiollisilla toimijoilla vaikuttaa olevan entistä suuremmat intressit päästä käsiksi suoraan teollisuusautomaatiojärjestelmien toimintaan.[43]

Jouni Pöyhösen väitöstutkimuksessa Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa – Systeemiajattelu, ja sen tausta-aineistona julkaistussa artikkelissa *Cyber Security Creation as Part of the Management of an Energy Company*[44], toteutettiin SWOT-analyysi. Analyysissä haastateltiin suomalaisia energiayhtiöitä ja kartoitettiin niiden kyberturvallisuuteen liittyviä vahvuuksia ja heikkouksia. Analyysin perusteella yhtiöt ovat yleisesti tunnistaneet tämän päivän kybertoimintaympäristön uhat ja suojautuneet melko hyvin tavanomaisia haittaohjelmia vastaan. Varsinkin isoilla yrityksillä on myös käytössään uusinta teknologiaa ja tietoturvayhtiöiden osaamista hyödynnetään laajasti.

Haasteita ja kehitettävää kuitenkin riittää. Yritysten on esimerkiksi vaikea suojautua edistyksellisempiä haittaohjelmia, APT (Advanced Persistent Threat) vastaan, ja reaaliaikaisen tilannekuvan ylläpitäminen monimutkaisissa tietojärjestelmissä on haastavaa. Kyberuhilta suojautuminen on edelleen paljolti reaktiivista, vaikka proaktiiviseen suuntaan ollaan pikkuhiljaa menossa. Yhtenä haasteena voidaan myös nähdä kyberturvallisuuden ja hyvien suojauskäytänteiden jalkauttaminen kaikille organisaation tasoille sekä toiminnan kannalta merkittävien sidosryhmien toimintaan.[45] Lisäksi pienemmissä yrityksissä

[43] Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus 2022.

[44] Pöyhönen, Jouni, – Lehto, Martti, Cyber security creation as part of the management of an energy company, ECCWS 2017: Proceedings of the 16th European Conference on Cyber Warfare and Security, s. 332–340. Academic Conferences and Publishing International Limited 2017.

[45] Pöyhönen 2020, s. 115–120.

kyberturvallisuuden huomioiminen ja suojaustoimenpiteet ovat selvästi jäljessä isommista yrityksistä.[46]

[46] Helsingin seudun kauppakamari 2019, s. 30.

3 Sähköverkkojen kyberturvallisuussääntely

3.1 Suomalainen kyberturvallisuussääntely

Suomen lainsäädännössä ei ole kyberturvallisuutta koskevaa yleislakia, josta löytyisi yleisiä, kaikkien eri alojen toimijoita velvoittavia säännöksiä. Sen sijaan kyberturvallisuusvelvoitteita löytyy jokaisen toimialan omasta erityislainsäädännöstä. Osa velvoitteista koskee viranomaisia ja osa yksityisiä toimijoita, joista monet voidaan katsoa kriittisiksi toimijoiksi.

Esimerkiksi energiahuoltoalalla kyberturvallisuutta tai yleistä turvallisuutta koskevia säännöksiä löytyy *sähkömarkkinalaista (588/2013)*, *maakaasumarkkinalaista (587/2017)* sekä *sähkö- ja maakaasumarkkinoiden valvonnasta annetusta laista (590/2013)*. Digitaalista infrastruktuuria koskevia säännöksiä löytyy puolestaan esimerkiksi *sähköisen viestinnän palveluista annetusta laista (917/2014)* ja terveydenhuoltoalaa koskevia velvoitteita *sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetusta laista (784/2021)* sekä *laista sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019)*. Finanssialalla velvoittavaa sääntelyä löytyy muun muassa *luottolaitostoiminnasta annetusta laista (610/2014)* sekä *maksulaitoslaista (297/2010)*.

Kyberturvallisuusvelvoitteiden hajauttaminen sektorikohtaiseen lainsäädäntöön on nähty toimivimpana ratkaisuna muun muassa siitä syystä, että eri toimialoilla on omat erityispiirteensä.[47] Ei olisi tarkoituksenmukaista tai toimivaa säätää yksityiskohtaisia velvoitteita, joita kaikkien toimijoiden eri aloilla olisi noudatettava. Lisäksi kyberturvallisuuden yleislakia ei ole haluttu säätää siitä syystä, että se voisi pahimmillaan monimutkaistaa sääntelyä, aiheuttaa päällekkäisyyttä sektorikohtaisen lainsäädännön kanssa, sekä aiheuttaa kohtuutonta hallinnollista taakkaa niin yrityksille kuin myös alan valvoville viranomaisille. Kyberturvallisuusvelvoitteiden liittämisellä sektorikohtaiseen lainsäädäntöön on tavoiteltu myös sitä, että toimijat mieltäisivät kyberturvallisuuden riskit ja niihin varautumisen kuuluvan osaksi yrityksen normaalia toimintaan ja yleistä riskienhallintaa, eikä joksikin muusta varautumisesta erilliseksi toiminnaksi.[48]

---

[47] Liikenne- ja viestintäministeriö 2021, s. 17.

[48] HE 192/2017 vp., s. 57.

Tässä kohtaa on mielenkiintoista hieman verrata Suomen valitsemaa lähestymistapaa esimerkiksi Iso-Britanniassa sekä Puolassa omaksuttuun oikeudelliseen linjaan. Kyseisissä maissa on nimittäin laadittu, jäljempänä käsiteltävän NIS-direktiivin implementoinnin yhteydessä, *kyberturvallisuuden yleislait*, joissa asetetaan velvoitteita kaikille kriittisille toimijoille.[49] Suomen valitsema linja vaikuttaa siis poikkeavan merkittävästi monista muista Euroopan maista.

Kriittisten toimialojen varautumisvelvoitteet ovat historiallisesti liittyneet enimmäkseen *fyysisen maailman uhkiin* tai *uhkiin yleisesti*. Sektorikohtaisesta lainsäädännöstämme onkin löytynyt jo pidemmän aikaa säännöksiä, joilla tietyt kriittiset toimijat on velvoitettu varautumaan erilaisiin poikkeusoloihin tai vakaviin normaaliolojen häiriötilanteisiin. Muun muassa sähkömarkkinalain 19 §:ssä määrätään, että sähköverkot on suunniteltava, rakennettava ja ylläpidettävä siten, että verkot toimivat mahdollisimman luotettavasti normaaliolojen häiriötilanteissa ja valmiuslaissa tarkoitetuissa poikkeusoloissa.

Tämänkaltaiset säännökset ovat kuitenkin olleet vanhastaan hyvin yleisluonteisia, eikä niissä ole annettu määräyksiä nimenomaan kyberturvallisuudesta huolehtimisesta. Vasta seuraavassa luvussa esiteltävän, vuonna 2016 annetun *EU:n verkko- ja tietoturvadirektiivin (NIS-direktiivi)*[50] myötä monille toimialoille, kuten energiahuoltoon saatiin omat, nimenomaisesti kyberturvallisuutta käsittelevät pykälät. Kriittisten toimialojen kyberturvallisuutta koskeva sääntely vaikuttaa siis kokonaisuudessaan olevan vielä kehitysvaiheessa, ja kybermaailman uhkiin ja niiden aiheuttamiin sääntelytarpeisiin ollaan sekä kansainvälisesti että kansallisesti vasta heräämässä.

Vuonna 2018 voimaan tullut *yleinen tietosuoja-asetus*[51] sisältää joitakin säännöksiä tietoturvasta. Esimerkiksi asetuksen toinen jakso käsittelee henkilötietojen turvallisuutta ja siinä määrätään henkilötietoja käsittelevälle rekisterinpitäjälle velvollisuus toteuttaa *asianmukaiset tekniset ja organisatoriset toimenpiteet* järjestelmiensä tietoturvallisuudesta

---

[49] Calder 2018, s. 11; Chałubińska-Jentkiewicz – Radoniewicz – Zieliński 2022, s. 93.

[50] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa, (Julkaistu Euroopan unionin virallisessa lehdessä 19.7.2016).

[51] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).

huolehtimiseksi. Lisäksi rekisterinpitäjällä on velvollisuus ilmoittaa järjestelmiinsä kohdistuneesta tietoturvaloukkauksesta valvontaviranomaiselle ja rekisteröidyille. Kyseiset säännökset ovat saman tyylisiä, kuin seuraavaksi esiteltävässä EU:n verkko- ja tietoturvadirektiivissä, mutta niitä ei käsitellä tässä tutkielmassa tarkemmin siitä syystä, että koko yleinen tietosuoja-asetus koskee nimenomaan luonnollisten henkilöiden *henkilötietojen suojelua*, eikä yleisemmin esimerkiksi kriittisten toimijoiden tietojärjestelmien kyberturvallisuutta.

3.2 Sähköverkkojen kyberturvallisuuden velvoitesääntely

3.2.1 Euroopan unionin sääntely

Merkittävin kriittisten toimijoiden kyberturvallisuutta koskeva EU-säädös on *EU:n verkko- ja tietoturvadirektiivi* (jäljempänä NIS-direktiivi). Lyhenne NIS tulee sanoista ”Directive on Security of *Network and Information Systems*”. Direktiivi on ensimmäinen koko EU:n laajuinen säädös, jossa annetaan yleiset vähimmäisvaatimukset kriittisten toimialojen organisaatioiden kyberturvallisuudelle.

Heti tämän luvun alkuun on hyvä tuoda ilmi, että EU on juuri tätä tutkielmaa viimeisteltäessä hyväksynyt uuden *kyberturvallisuusdirektiivin* (jäljempänä NIS2 -direktiivi).[52] Kyseisen päivityksen myötä, kaikkien kriittisten toimialojen kyberturvallisuuden vähimmäisvaatimukset tulevat täsmentymään ja tiukentumaan huomattavasti. Tämä tutkielma pohjautuu alkuperäiseen NIS-direktiiviin, sillä se on virallisesti voimassa vielä 18.10.2024 asti, jolloin NIS2 -direktiivin implementointiaika päättyy. Uusi direktiivi on kuitenkin huomioitu tutkimuksessa, ja sen myötä tulevia uudistuksia tarkastellaan vielä laajemmin luvussa 5.2.

Jotta NIS-direktiiviä ja sen velvoitteita pystyttäisiin juridisesti pätevällä tavalla arvioimaan, on heti alkuun hyvä hieman yleisesti tarkastella EU-direktiivien luonnetta, velvoittavuutta ja suhdetta kansalliseen lainsäädäntöön. Direktiivit määritellään *Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT)* 288 artiklassa, jonka mukaisesti direktiivi velvoittaa saavutettavaan tulokseen nähden, mutta jättää kansallisten viranomaisten valittavaksi muodon

[52] Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta.

ja keinot. Toisin kuin *EU-asetukset*, direktiivit eivät siis ole jäsenvaltioissa suoraan sovellettavaa oikeutta, vaan ne tulee panna täytäntöön kansallisen lainsäädännön kautta. Näin ollen myös direktiiveissä asetetut velvoitteet tulee lainsoveltamistilanteissa lähtökohtaisesti johtaa kansallisesta lainsäädännöstä. Suomessa sähköverkonhaltijoita koskevat NIS-direktiivin velvoitteet on pantu täytäntöön *sähkömarkkinalailla*; tätä käsitellään tarkemmin luvussa 3.2.5.

Euroopan unionin tuomioistuimen oikeuskäytännössä syntyneet *oikeusperiaatteet* auttavat täsmentämään direktiivien ja kansallisen lainsäädännön välistä suhdetta. Ensinnäkin *ensisijaisuusperiaatteen* mukaisesti, eurooppaoikeus syrjäyttää kansallisen lain, mikäli niiden välillä on ristiriita.[53] Periaate on yleisesti tunnustettu ja se on vakiintunut yhdeksi koko EU:n oikeusjärjestelmän olemassaolon perustaksi. Ensisijaisuusperiaatteen toteutuminen käytännössä ei ole kuitenkaan täysin suoraviivaista, ja etenkin direktiivien kohdalla on huomioitava myös muita periaatteita.

Eurooppaoikeuden *välittömän vaikutuksen periaatteen* mukaan, tietyillä EU-säädöksillä on kansallisessa oikeusjärjestelmässä välitön vaikutus, ja luonnollinen henkilö tai oikeushenkilö voi kansallisessa tuomioistuimessa vedota suoraan tähän eurooppaoikeudelliseen säädökseen.[54] Direktiivit eivät voi luonteestaan johtuen saada kokonaisuudessaan välittömiä vaikutuksia, mutta sen sijaan niiden *yksittäiset, riittävän täsmälliset ja ehdottomat artiklat* voivat tulla joissakin tapauksissa myös välittömästi vaikuttaviksi.[55]

Välitön vaikutus voidaan edelleen jakaa *vertikaaliseen välittömään vaikutukseen* (valtion ja yksityisen välinen tilanne) ja *horisontaaliseen välittömään vaikutukseen* (kahden yksityisen tahon välinen tilanne). Vertikaalinen välitön vaikutus kuvaa tilannetta, jossa EU-säädös luo velvoitteita nimenomaan jäsenvaltioille. Direktiiveillä voi olla tällainen vertikaalinen välitön vaikutus, sillä ne on osoitettu jäsenvaltioille, ja niiden mukaiset velvoitteet aktualisoituvat jäsenvaltion välityksellä yksityisille tahoille, kun direktiivin velvoitteet implementoidaan osaksi kansallista lainsäädäntöä.

---

[53] Raitio – Tuominen 2020, s. 234.

[54] Raitio – Tuominen 2020, s. 242.

[55] Raitio – Tuominen 2020, s. 247.

Horisontaalinen välitön vaikutus kuvaa puolestaan tilannetta, jossa EU-säädös luo velvoitteita suoraan yksityisille toimijoille, suhteessa toisiin yksityisiin toimijoihin. Direktiiveillä ei voi luonteestaan johtuen olla horisontaalista välitöntä vaikutusta. Tämä voi johtaa käytännössä ongelmalliseen tilanteeseen, jossa yksityistä toimijaa ei voida asettaa vastuuseen direktiivin velvoitteiden noudattamatta jättämisestä, mikäli jäsenvaltio ei ole onnistunut direktiivin implementoimisessa, ja tästä syystä kansallinen lainsäädäntö on jäänyt puutteelliseksi.[56]

Horisontaalisen välittömän vaikutuksen kielto voi siis aiheuttaa käytännön ongelmia direktiivin tavoitteiden toteutumiselle, mistä syystä EU-tuomioistuimen oikeuskäytännössä on ongelman lievittämiseksi omaksuttu myös niin sanottu *yhdenmukaisen tulkinnan periaate*. Sen mukaan kansallista lainsäädäntöä tulee tulkita mahdollisimman yhdenmukaisesti EU-säädösten sekä integraatiotavoitteiden kanssa. Yhdenmukaisella tulkinnalla pyritään takaamaan EU-direktiivien tehokkuus ja niiden asettamien päämäärien saavuttaminen.[57]

Edellä esitettyjen periaatteiden valossa, NIS-direktiivi velvoittaa nimenomaan jäsenvaltioita varmistamaan, että direktiivin soveltamisalaan kuuluvat kriittiset toimijat omaksuvat direktiivin mukaiset kyberturvallisuuden vähimmäisvaatimukset. Lakiteknisesti nämä velvoitteet tulee johtaa lainsoveltamistilanteessa kansallisesta lainsäädännöstä, joka sähköverkonhaltijoiden yhteydessä tarkoittaa sähkömarkkinalakia.

Vaikka NIS-direktiivi saakin käytännön vaikutuksensa kansallisen lainsäädännön kautta, on sitä silti mielekästä käsitellä myös itsenäisesti, muun muassa edellä esitetystä yhdenmukaisen tulkinnan periaatteesta johtuen. Näin päästään paremmin käsiksi direktiivin säännösten tarkkaan merkitykseen, velvoittavuuteen ja direktiivin tavoitteisiin. Kun tämän jälkeen tarkastellaan kansallista lainsäädäntöä, voidaan tätä verrata NIS-direktiiviin ja arvioida, miten hyvin lainsäätäjä on onnistunut direktiivin implementoimisessa. NIS-direktiivi ja sähkömarkkinalain relevantit pykälät on siis hyvä ymmärtää yhdeksi erottamattomaksi kokonaisuudeksi.

---

[56] Raitio – Tuominen 2020, s. 245.

[57] Raitio – Tuominen 2020, s. 252–253.

3.2.2 NIS-direktiivin kyberturvallisuusriskien hallintaan liittyvät velvoitteet

NIS-direktiivin pääasiallisena sisältönä ovat: 1) kriittisille toimijoille asetettavat kyberturvallisuusriskienhallinnan vähimmäisvaatimukset, 2) vaatimus ilmoittaa merkittävistä kyberturvallisuuden poikkeamista viranomaisille, 3) jäsenvaltioiden velvollisuus hyväksyä verkko- ja tietojärjestelmien turvallisuutta koskeva kansallinen strategia sekä 4) jäsenvaltioiden velvollisuus nimetä direktiivin mukaiset *kansalliset toimivaltaiset viranomaiset*, yksi viranomainen *kansalliseksi keskitetyksi yhteyspisteeksi* sekä yksi tai useampi viranomainen kansalliseksi *CSIRT-toimijaksi* (Computer Security Incident Response Team). Viranomaisia koskevia NIS-direktiivin määräyksiä käsitellään tarkemmin luvussa 3.3.

Kriittisistä toimijoista käytetään NIS-direktiivissä käsitettä *keskeisten palvelujen tarjoajat*. Kriteerit keskeisten palvelujen tarjoajien määrittelemiseksi annetaan 5 artiklan toisessa kohdassa:

> a) toimija tarjoaa palvelua, joka on keskeinen yhteiskunnan ja/tai talouden kriittisten toimintojen ylläpitämiseksi, b) kyseisen palvelun tarjoaminen on riippuvainen verkko- ja tietojärjestelmistä, ja c) poikkeamalla olisi merkittäviä haitallisia vaikutuksia kyseisen palvelun tarjoamiseen.

Tämän lisäksi määritelmää tarkennetaan direktiivin liitteessä II, jossa kaikki direktiivin soveltamisalaan kuuluvat kriittiset toimialat sekä toimialoja täsmentävät osa-alueet on lueteltu taulukossa. Toimialoja ovat muun muassa energia, liikenne, pankkiala ja terveydenhuoltoala. Sähkö on määritelty yhdeksi energiatoimialan osa-alueeksi, minkä lisäksi taulukossa on mainittu esimerkkejä osa-alueiden toimijoista. Näistä toimijoista on mainittu *sähköalan yritykset*, *jakeluverkonhaltijat* ja *siirtoverkonhaltijat*. NIS-direktiiviä sovelletaan siis yleisesti sähköverkonhaltijoihin.

NIS-direktiivin merkittävimmät, kyberturvallisuusriskien hallintaan liittyvät velvoitesäännökset löytyvät direktiivin 14 artiklasta, ja niiden mukaan:

> 1. Jäsenvaltioiden on varmistettava, että keskeisten palvelujen tarjoajat toteuttavat asianmukaiset ja oikeasuhteiset tekniset ja organisatoriset toimenpiteet hallitakseen riskejä, joita kohdistuu niiden verkko- ja tietojärjestelmien turvallisuuteen, joita nämä keskeisten palvelujen tarjoajat käyttävät toiminnoissaan. Näillä toimenpiteillä on varmistettava riskiin suhteutettu verkko- ja tietojärjestelmien turvallisuuden taso uusin tekniikka huomioon ottaen.
>
> 2. Jäsenvaltioiden on varmistettava, että keskeisten palvelujen tarjoajat toteuttavat asianmukaiset toimenpiteet, joilla ehkäistään ja minimoidaan tällaisten keskeisten

> palvelujen tarjoamisessa käytettyjen verkko- ja tietojärjestelmien turvallisuuteen vaikuttavien poikkeamien vaikutus näiden palvelujen jatkuvuuden takaamiseksi.

Säännös on direktiiveille tyypilliseen tapaan yleisluonteinen, sillä sen sisältämät velvoitteet on tarkoitus määritellä tarkemmin kansallisessa lainsäädännössä. Kovin paljoa yksityiskohtaisemmat määräykset eivät olisi myöskään tarkoituksenmukaisia, sillä direktiivi kattaa niin suuren kirjon erilaisia toimialoja ja toimijoita, että niiden väliset eroavaisuudet vaikuttaisivat epäilemättä yksityiskohtaisemman sääntelyn toimivuuteen.

Kuten luvussa 3.1 todettiin, Suomessa ei ole kansallisella tasolla yhtä keskitettyä kyberturvallisuuslakia, vaan NIS-direktiivin määräykset toteutuvat kunkin kriittisen toimialan oman erityislainsäädännön kautta. Tämä on katsottu parhaaksi vaihtoehdoksi muun muassa siitä syystä, että kyberturvallisuussäännöksiä on jo ennen direktiivin voimaantuloa löytynyt joidenkin alojen lainsäädännöstä, eikä direktiivin implementoinnilla ole haluttu lisätä turhaa sääntelyä tai päällekkäisyyttä.[58]

Yleisluonteisuudestaan huolimatta, NIS-direktiivin 14 artiklasta voidaan löytää selkeitä viitteitä siitä, millaisia toimenpiteitä kriittisiltä toimijoilta edellytetään. Nämä velvoitteet ovat tutkielman ytimessä ja seuraavaksi avataan tulkintoja 14 artiklan sisällöstä.

Oikeustieteessä vakiintuneiden tulkintateorioiden mukaan, säännöksen tulkintaa voidaan lähestyä esimerkiksi sen *kielellisen ilmaisun kautta*. Kyseisessä, *semanttisessa tulkintateoriassa* painotetaan säännöksen semanttisen eli kielellisen merkityksen selvittämistä.[59] Sanamuodon mukainen tulkinta on katsottu myös EU-oikeudessa ensisijaiseksi tulkintateoriaksi.[60] NIS-direktiivin kontekstissa on siis merkityksellistä selvittää, mitä 14 artiklassa esitetyillä ilmaisuilla tarkoitetaan, jotta niiden yksittäisille toimijoille asettamat velvoitteet pystyttäisiin määrittelemään.

Semanttisen tulkintateorian mukaan, jonkin käsitteen merkitys voidaan määrittää ensinnäkin viittaamalla sen yleiskielen mukaiseen merkitykseen sekä termin käyttöön sen tavanomaisissa kielenkäyttöyhteyksissä.[61] Direktiivin 14 artiklassa edellytetään jäsenvaltioiden varmistavan,

---

[58] Liikenne- ja viestintäministeriö 2017, s. 29.
[59] Siltala 2003, s. 334.

[60] Talus – Penttinen 2016, s. 237

[61] Siltala 2003, s. 335.

että toimijat toteuttavat *asianmukaiset ja oikeasuhteiset tekniset ja organisatoriset toimenpiteet* hallitakseen kyberturvallisuuden riskejä. Asianmukaisuudella voitaisiin tarkoittaa esimerkiksi sitä, että toimenpiteiden tulisi olla ”riittäviä” huomioiden kunkin kriittisen toimialan olosuhteet, yleiset käytännöt ja hyvät toimintatavat.

Semanttisessa tulkintateoriassa käsitteitä voidaan arvioida myös niiden *juridis-teknisessä erityismerkityksessä*, jolloin tulkinta sidotaan juristien kielelliseen ja ammatilliseen itseymmärrykseen.[62] Artiklan ilmaisun *oikeasuhtaisuus* merkitystä voitaisiin näin ollen lähestyä esimerkiksi sitä kautta, millaisia toimia kyberuhkien torjumiseksi pidettäisiin todennäköisimmin oikeasuhtaisina, mikäli asiaa puitaisiin oikeudessa, ja millaisia merkityksiä juristit siellä käsitteelle antaisivat. Tässä esimerkkitapauksessa tulkinnat olisivat kuitenkin epäilemättä hyvin tilannesidonnaisia, ja 14 artiklan mukaisten toimenpiteiden oikeasuhtaisuutta jouduttaisiinkin todennäköisesti joka tapauksessa arvioimaan käyttämällä apuna myös muuta, kuin semanttista tulkintateoriaa.

Artiklan mainitsemat *tekniset toimenpiteet* viittaavat epäilemättä kriittisten toimijoiden tietojärjestelmien teknisiin ratkaisuihin, kuten kyberturvallisuuden huomioiviin ja turvallisiin järjestelmäarkkitehtuureihin sekä erilaisiin suojaus- ja valvontaohjelmiin. *Organisatoriset toimenpiteet* viittaavat puolestaan organisaatioissa omaksuttuihin toimintatapoihin, joilla on merkitystä kyberturvallisuuden kannalta. Tällaiset toimintatavat voisivat tarkoittaa esimerkiksi henkilöstöltä vaadittavaa kyberturvallisuusosaamisen tasoa tai pääsynhallintakäytänteitä. Myös aihetta käsittelevässä aiemmassa tutkimuksessa on päädytty samantyyliseen tulkintaan 14 artiklan mukaisista kyberturvallisuustoimenpiteistä.[63]

Toimenpiteiden toteutuksessa on lisäksi huomioitava *uusin tekniikka*, mikä vaikuttaa itseasiassa semanttisen tulkintateorian valossa hyvin ankaralta määräykseltä. Ilmaisu uusin tekniikka on toki hyvin yleinen, mutta se antaa viitteitä siitä, että toimijat olisivat velvollisia jatkuvasti päivittämään järjestelmiään ja kehittämään kyberuhkiin varautumista organisaatiossaan. Jouni Pöyhösen väitöstutkimuksessa Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa – Systeemiajattelu, kuvataan hyvin yksityiskohtaisesti nykyisin käytössä olevia teknisiä ratkaisuja

---

[62] Siltala 2003, s. 336.

[63] Lahti 2022, s. 44.

kyberturvallisuudesta huolehtimiseksi.[64] Nämä ratkaisut myös kehittyvät teknisesti koko ajan, joten mikäli direktiivin 14 artiklaa tulkittaisiin ankarasti, toimijat voisivat sen perusteella olla velvoitettuja hyvinkin mittaviin ja jatkuviin teknisiin investointeihin.

Tähän väliin on kiinnostavaa tarkastella kyseisen ilmaisun esiintymistä direktiivin implementoinnin yhteydessä. On yllättävää, että ilmaisuun ei oteta mitään kantaa esimerkiksi NIS-direktiivin implementointiin liittyvässä hallituksen esityksessä.[65] Vaatimukseen uusimman tekniikan huomioimisesta ei myöskään enää viitata sähkömarkkinalain 29 a §:ssä, jolla direktiivin 14 artikla on implementoitu kansallisesti. Vaikuttaa siis siltä, että kyseinen, potentiaalisesti hyvinkin vahvasti velvoittava ilmaisu on kokonaan sivuutettu NIS-direktiivin kansallisessa täytäntöönpanossa.

Tässä yhteydessä voidaan vielä todeta, että uusimman tekniikan vaatimus on mitä ilmeisimmin nähty sellaisenaan liian ankarana ilmaisuna myös EU-tasolla, kun NIS-direktiivin säännöksiä on tarkasteltu uudelleen direktiivin uudistustyön yhteydessä. Uudessa NIS2 -direktiivissä ei nimittäin enää puhuta uusimman tekniikan vaatimuksesta, vaan sen tilalle on otettu yleisluonteisempi vaatimus huomioida *viimeisin kehitys* ja tapauksen mukaan asiaa koskevat eurooppalaiset ja kansainväliset standardit, sekä täytäntöönpanokustannukset. Artiklatekstissä ei siis enää korosteta nimenomaisesti uusinta *tekniikkaa*, minkä lisäksi *viimeisimmän kehityksen* vastapainoksi on otettu *täytäntöönpanokustannukset*.

Direktiivin johdanto-osassa tarkennetaan 14 artiklan soveltamisalaa muun muassa siten, että toimijat ovat vastuussa kyberuhkiin varautumisesta siitäkin huolimatta, että niiden käyttämät tietojärjestelmät tai näiden järjestelmien tietoturvasta huolehtiminen olisi ulkoistettu jollekin toiselle toimijalle. Näin ollen NIS-direktiivin mukaan, esimerkiksi sähköverkonhaltija on vastuussa järjestelmiensä kyberturvallisuudesta, vaikka se olisi ulkoistanut järjestelmien tietoturvasta huolehtimisen jollekin ulkopuoliselle tietoturvayhtiöllä. Tämä on merkittävä huomio, kun ajatellaan toimijoiden vastuun jakautumista ongelmatilanteissa. NIS-direktiivi ei tosin näiltä osin vastaa kysymykseen siitä, miten esimerkiksi verkonhaltijan ja tietoturvayhtiön välinen sopimus vaikuttaisi vastuun jakautumiseen toimijoiden välillä.

---

[64] Pöyhönen 2020, s. 152–156.

[65] HE 192/2017 vp.

Samassa 14 artiklassa mainitaan toisaalta myös, että verkko- ja tietojärjestelmien turvallisuuden taso tulee suhteuttaa *riskiin*. Tämä on eittämättä tietynlainen myönnytys vaadittaville toimille, sillä sen perusteella kriittisiltä toimijoilta vaadittavia toimenpiteitä tulisi aina arvioida sen perusteella, millaisia uhkia niiden toimintaan todellisuudessa kohdistuu. Esimerkiksi sähköverkonhaltijoiden tulisi mitoittaa toimensa sen mukaan, millaisia kyberhyökkäyksiä niiden käyttämiin tietojärjestelmiin ja tietoverkkoihin tyypillisesti kohdistetaan. Esimerkiksi ETSI (European Telecommunications Standards Institute) on NIS-direktiivin implementointiin liittyvässä raportissaan ottanut kantaa riskiarviointien tekemiseen organisaatiossa ja korostanut, että arvioinneissa olisi myös aina kohtuullista huomioida kullakin organisaatiolla riskienhallintaan käytettävissä olevat resurssit.[66]

Direktiivin johdanto-osassa täsmennetään myös, että toimijoilta edellytettävien toimenpiteiden ei tulisi aiheuttaa *suhteetonta taloudellista ja hallinnollista rasitusta*. Täsmennys on edelleen eräänlainen myönnytys vaadittaville toimille, ja sen mukaan toimijoiden ei olisi varauduttava käyttämään ylettömiä määriä rahaa ja vaivaa kyberturvallisuudesta huolehtimiseksi.

Liikenne- ja viestintäministeriön laatimassa raportissa *Tietoturvan ja tietosuojan parantamisesta yhteiskunnan kriittisillä toimialoilla*, käsitellään ristiriitaa, joka vallitsee riittävien kyberturvallisuustoimien ja toisaalta näiden aiheuttamien kustannusten välillä.[67] Organisaatioilla on usein kannustinongelmia investoida riittävään kyberturvallisuuden tasoon, sillä investoinnit aiheuttavat välittömiä taloudellisia kustannuksia, joista saatavat hyödyt ovat epäselviä. Mikäli organisaation järjestelmiin ei kohdistetakaan kyberhyökkäyksiä, tietoturvainvestointien voidaan helposti ajatella olleen ”turhia”. Kannustinongelmaa voi myös lisätä se, että toimijat eivät joudu useinkaan kantamaan itse kaikkia kyberhyökkäyksestä syntyneitä kustannuksia, vaan osa niistä ohjautuu asiakkaiden tai yhteiskunnan maksettavaksi.[68] Kuitenkin investointi voi hyökkäyksen sattuessa osoittautua erittäin kannattavaksi sekä välittömässä rahallisessa arvossa että mainehaittojen torjumisen kannalta.

Semanttisen tulkintateorian lisäksi, oikeussäännön tulkinnassa voidaan keskittyä myös esimerkiksi siihen, mikä on sen *tarkoitus tai päämäärä*. Tällöin puhutaan oikeussäännön

---

[66] ETSI 2017, s. 18.

[67] Liikenne- ja viestintäministeriö 2021, s. 21–27.
[68] Sales 2013, s. 1526–1527.

teleologisesta tulkinnasta. Euroopan unionin oikeudessa suositaan teleologista tulkintaa, minkä lisäksi se sopii hyvin tilainteisiin, joissa itse säänneltävä toimintaympäristö on muutoksessa.[69] Näin ollen myös NIS-direktiivin tarkasteleminen teleologisen tulkintateorian valossa on luontevaa, sillä myös sääntelyn kohteena oleva kyberympäristö muuttuu koko ajan.

NIS-direktiivin tavoite tuodaan sanallisesti ilmi direktiivin johdanto-osan 74 kappaleessa, jonka mukaan direktiivin tavoitteena on *yhteinen korkeatasoinen verkko- ja tietojärjestelmien turvallisuus koko unionin tasolla*. Voidaan ajatella, että teleologisen tulkintateorian valossa vaatimus verkko- ja tietojärjestelmien *korkeasta tasosta* korostaa entisestään vaatimusta siitä, että jäsenvaltioiden on luotava sellaiset kansalliset säännökset, jotka todella velvoittavat kriittiset toimijat huolehtimaan laadukkaista kyberturvallisuusratkaisuista organisaatioissaan.

Itse 14 artiklasta voidaan löytää muutamia nimenomaisia tavoitteita. Varautumistoimenpiteiden on esimerkiksi *taattava palveluiden jatkuvuus*. Ilmaisu korostaa sitä, että kyberturvallisuus ja riskienhallinta on kyettävä hoitamaan niin hyvin, että palvelut eivät keskeytyisi mahdollisen kyberhyökkäyksen sattuessa. Lisäksi vaadittavia kyberturvallisuustoimenpiteitä tarkennetaan 14 artiklan toisessa kohdassa siten, että niiden on *ehkäistävä* ja *minimoitava* kyberturvallisuuden poikkeamien vaikutuksia. Myös tämä ilmaisu korostaa vaatimusta, jonka mukaan teknisten ratkaisujen ja omaksuttujen toimintatapojen on oltava myös todellisuudessa niin hyviä, että niiden avulla voidaan ehkäistä ja minimoida kyberhyökkäysten aiheuttamia vahinkoja. Kaiken kaikkiaan voidaan kuitenkin argumentoida, että koska myös NIS-direktiivistä löydettävissä olevat tavoitteet on ilmaistu hyvin yleisellä tasolla, ei direktiivin tarkastelemisella teleologisen tulkintateorian valossa voida saada kovin paljoa tulkinnallista apua direktiivin velvoitteiden määrittelemiseen.

3.2.3 NIS-direktiivin poikkeamailmoituksiin liittyvät velvoitteet

Edellä käsiteltyjen, kyberturvallisuusriskien hallintaan liittyvien säännösten lisäksi, NIS-direktiivin 14 artiklassa määrätään myös *toimijoiden velvollisuudesta ilmoittaa valvoville viranomaisille merkittävistä kyberturvallisuuden poikkeamista*. Artiklan kolmannen ja neljännen kohdan mukaan:

> 3. Jäsenvaltioiden on varmistettava, että keskeisten palvelujen tarjoajat ilmoittavat ilman aiheetonta viivytystä toimivaltaiselle viranomaiselle tai CSIRT-toimijalle

[69] Talus – Penttinen 2016, s. 241.

> poikkeamista, joilla on merkittävä vaikutus niiden tarjoamien keskeisten palvelujen jatkuvuuteen. Ilmoituksiin on sisällytettävä tiedot, joiden perusteella toimivaltainen viranomainen tai CSIRT-toimija voi määrittää poikkeaman mahdollisen rajat ylittävän vaikutuksen. Ilmoittaminen ei lisää ilmoituksen tekevän osapuolen vastuuta.
>
> 4. Poikkeaman vaikutuksen merkittävyyden määrittämiseksi on otettava huomioon erityisesti seuraavat parametrit: a) niiden käyttäjien lukumäärä, joihin keskeisen palvelun häiriö vaikuttaa, b) poikkeaman kesto ja c) maantieteellinen levinneisyys alueella, johon poikkeama vaikuttaa.

Nämä säännökset vaikuttavat hieman selkeämmiltä, kuin edellä käsitellyt artiklan ensimmäinen ja toinen kohta, eikä niiden merkityksen selvittämisessä vaadita välttämättä samanlaista teoreettista pohdintaa ja tulkintaa. Näkemyksen puolesta puhuu esimerkiksi se, että ilmoitusvelvollisuuteen liittyvät säännökset on implementoitu eri toimialoille yhtenäisemmin, kuin kyberturvallisuusriskien hallintaan liittyvät verrokkinsa.[70]

Ilmoitusvelvollisuuteen liittyvät säännökset ovat tärkeä osa NIS-direktiiviä, ja niiden tarkoituksena on välittää ja pitää yllä kyberturvallisuuden tilannekuvaa. Juuri tilannekuvan kehittäminen on nähty yhtenä merkittävänä kehityskohteena suomalaisessa kyberturvallisuuskeskustelussa.[71]

Säännöksissä viitataan *toimivaltaiseen viranomaiseen* ja *CSIRT-toimijaan*, joille kyberuhan kohteena olevan toimijan on ilmoitettava poikkeamasta. Sähköverkonhaltijoiden osalta toimivaltaisena viranomaisena toimii *Energiavirasto* ja CSIRT-toimijana Suomessa yleisesti Liikenne- ja viestintäviraston *Kyberturvallisuuskeskus*.

Säännöksissä mainitulla ”poikkeamalla” tarkoitetaan 4 artiklan mukaan *mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti verkko- ja tietojärjestelmien turvallisuuteen*. Jos siis esimerkiksi sähköverkkoja hallinnoiviin järjestelmiin kohdistetaan kyberhyökkäys, jolla on merkittävä vaikutus sähköverkon toimivuuteen, verkonhaltijan on direktiivin mukaan ilmoitettava hyökkäyksestä ilman aiheetonta viivytystä Energiavirastolle tai Kyberturvallisuuskeskukselle.

Poikkeaman merkittävyyden arviointi jää käytännössä kunkin kriittisen toimijan oman harkinnan varaan. Kuitenkin, 14 artiklan seitsemännen kohdan mukaan, kunkin alan

---

[70] Liikenne- ja viestintäministeriö 2021, s. 28.

[71] Valtioneuvosto 2021, s. 14.

toimivaltaiselle viranomaiselle ja 11 artiklan mukaiselle *yhteistyöryhmälle* on annettu valtaa *kehittää ja hyväksyä suuntaviivoja* ilmoitusta edellyttävien olosuhteiden toteamiseksi. Suomessa Energiavirasto onkin antanut täsmentävän ohjeen poikkeamailmoituksen tekemisestä. Ohjetta käsitellään tarkemmin luvussa 3.2.5.

Yhteenvedon omaisesti voidaan todeta, että NIS-direktiivillä kyllä tavoitellaan kriittisten toimijoiden melko korkeaa kyberturvallisuuden tasoa ja tähän myös periaatteessa velvoitetaan. Nykyisellään direktiivi jättää kuitenkin kyberturvallisuusriskien hallintaan liittyvien toimenpiteiden *käytännön toteutuksen* hyvin avoimeksi. Direktiivissä ei esimerkiksi täsmennetä edes yleisellä tasolla, millaisia teknisten tai organisatoristen toimenpiteiden tulisi käytännössä olla. Myös aikaisemmassa asiaan liittyvässä tutkimuksessa on päädytty samaan näkemykseen direktiivin epämääräisyydestä.[72]

NIS-direktiivin kansallista täytäntöönpanoa tukeva työryhmä on loppuraportissaan ottanut kantaa direktiivin käytännön velvoittavuuteen ja tullut myöskin siihen samaan johtopäätökseen, että direktiivin mukaiset vähimmäisvelvoitteet eivät käy artikloista selvästi ilmi.[73] Lisäksi, kuten seuraavissa luvuissa tarkemmin kuvataan, lainsäätäjä on direktiivin implementointivaiheessa ottanut sen tulkintanäkökannan, että direktiivin määräyksen jättävät kriittisille toimijoille *vapauden valita käytännön keinot* kyberturvallisuudesta huolehtimiseksi.[74]

Näin ollen ei voitane perustellusti argumentoida, että mikään direktiivin säännöksistä olisi *riittävän täsmällinen tai ehdoton*, jotta niiden voitaisiin katsoa olevan *välittömästi vaikuttavia* kansallisella tasolla. Lisäksi direktiivin välittömän horisontaalisen vaikutuksen kiellosta johtuen, direktiivin velvoitteita ei voitaisi muutenkaan kansallisessa lainkäyttötilanteessa kohdistaa suoraan kriittisiin toimijoihin, vaan direktiivi velvoittaa suoraan vain jäsenvaltioita.

Edellä mainituista seikoista johtuen, direktiivin mukaisia velvoitteita arvioitaessa, joudutaan mitä todennäköisimmin turvautumaan viimesijaiseen EU-oikeudelliseen periaatteeseen, eli *yhdenmukaisen tulkinnan periaatteeseen.* Kun tarkastellaan sähköverkonhaltijoihin kohdistuvia NIS-direktiivin velvoitteita, olisi ne käytännössä johdettava sähkömarkkinalain

---

[72] Lahti 2022, s. 48.

[73] Liikenne- ja viestintäministeriö 2017, s. 35.

[74] HE 192/2017 vp., s. 59.

relevateista pykälistä niin, että näitä säännöksiä pyrittäisiin tulkitsemaan mahdollisimman yhdenmukaisesti NIS-direktiivin määräysten kanssa. Uutta NIS2 -direktiiviä ei ole vielä implementoitu, mutta siitäkin huolimatta se voi jo saada kansallisen sääntelyn tulkintaa ohjaavaa vaikutusta.[75] Asiaan palataan lyhyesti luvussa 3.2.5 sähkömarkkinalain tarkastelun yhteydessä.

Koska itse NIS-direktiivi on sisällöltään niin yleisluonteinen, jäsenvaltioille on jäänyt merkittävä vastuu direktiivin tavoitteiden toteuttamisessa ja sen mukaisten velvoitteiden asianmukaisessa implementoimisessa kansalliseen lainsäädäntöön. Seuraavissa luvuissa tutustutaan tähän kansalliseen sääntelyyn ja arvioidaan myös sitä, miten Suomi on onnistunut NIS-direktiivin implementoimisessa.

3.2.4 Sähkömarkkinalain yleiset velvoitteet sähköverkkojen turvallisuudesta

Kuten jo edellisessä luvussa todettiin, sähköverkonhaltijoita koskevat kansalliset kyberturvallisuuden velvoitesäännökset löytyvät pääosin *sähkömarkkinalaista*. Sähkömarkkinalaki käsittelee nimensä mukaisesti sähkömarkkinoita kokonaisuudessaan, ja laissa määrätään muun muassa sähköverkkotoiminnan luvanvaraisuudesta, verkonhaltijoiden velvollisuuksista sekä sähkösopimuksista. Sähköverkkojen turvallisuuteen liittyvät säännökset ovat siis vain osa lakia.

Sähkömarkkinalain 3 §:n ensimmäisessä kohdassa määritellään sähköverkon käsite seuraavasti:

> Tässä laissa tarkoitetaan *sähköverkolla* toisiinsa liitetyistä sähköjohdoista, sähköasemista sekä sähköverkon käyttöä ja sähköverkkopalveluiden tuottamista palvelevista muista sähkölaitteista ja sähkölaitteistoista, *järjestelmistä ja ohjelmistoista* muodostettua kokonaisuutta, joka on tarkoitettu sähkön siirtoon tai jakeluun.

Kyseisestä lainkohdasta käy siis ilmi, että myös *järjestelmät* ja *ohjelmistot* luetaan osaksi sähköverkkoja ja niiden toimintaa. Määritelmä on syytä huomioida, kun tarkastellaan sähkömarkkinalain muita pykäliä, joissa asetetaan sähköverkoille yleisiä turvallisuuteen ja laatuun liittyviä vaatimuksia. Seuraavaksi käsitellään sähkömarkkinalain 19 §:ää ja arvioidaan, voitaisiinko pykälästä johtaa välillisesti myös kyberturvallisuusvelvoitteita.

---

[75] Raitio – Tuominen 2020, s. 254.

Sähkömarkkinalain 19 §:ssä säädetään verkonhaltijan velvollisuudesta kehittää hallitsemaansa verkkoa sekä varmistaa sen turvallisuus ja sähköntoimituksen laatu:

> Verkonhaltijan tulee riittävän hyvälaatuisen sähkön saannin turvaamiseksi verkkonsa käyttäjille ylläpitää, käyttää ja kehittää sähköverkkoaan sekä yhteyksiä toisiin verkkoihin sähköverkkojen toiminnalle säädettyjen vaatimusten ja verkon käyttäjien kohtuullisten tarpeiden mukaisesti.
>
> Sähköverkko on suunniteltava ja rakennettava ja sitä on ylläpidettävä siten, että:
>
> 1) sähköverkko täyttää sähköverkon toiminnan laatuvaatimukset ja sähkönsiirron sekä -jakelun tekninen laatu on muutoinkin hyvä;
>
> 2) sähköverkko ja sähköverkkopalvelut toimivat luotettavasti ja varmasti silloin, kun niihin kohdistuu normaaleja odotettavissa olevia ilmastollisia, mekaanisia tai muita ulkoisia häiriöitä;
>
> 3) sähköverkko ja sähköverkkopalvelut toimivat mahdollisimman luotettavasti normaaliolojen häiriötilanteissa ja valmiuslaissa (1552/2011) tarkoitetuissa poikkeusoloissa;
>
> …

Pykälän ensimmäinen momentti sekä toisen momentin ensimmäinen kohta ovat luonteeltaan yleisiä velvoitteita varmistaa sähköverkkojen turvallisuus ja sähköntoimituksen laatu, eivätkä ne varsinaisesti täsmennä tai konkretisoi vaadittavia toimia. Ensimmäisessä momentissa vain viitataan sähköverkkojen toiminnalle säädettyihin laatuvaatimuksiin ja verkon käyttäjien kohtuullisiin tarpeisiin. Sähkömarkkinalain hallituksen esityksen mukaan nämä toiminnalle säädettävät laatuvaatimukset määräytyvät tarkemmin muualla sähkömarkkinalaissa.[76] Tarkemmin laatuvaatimuksista säädetään kantaverkon osalta 40 ja 41 §:ssä, suurjännitteisten jakeluverkkojen osalta 50 §:ssä sekä jakeluverkkojen osalta 51 ja 52 §:ssä. Nämäkin pykälät ovat luonteeltaan melko yleisiä, eikä niissä oteta nimenomaisesti kantaa esimerkiksi sähköverkkoja hallinnoivien tietojärjestelmien- ja verkkojen kyberturvallisuuteen.

Sähkömarkkinalain 19 §:n toisen momentin toisessa kohdassa mainitaan *muut odotettavissa olevat ulkoiset häiriöt*, joiden sattuessa sähköverkkojen ja sähköverkkopalveluiden tulisi toimia luotettavasti ja varmasti. Lain esitöiden mukaan säännöksen soveltuvuutta arvioitaessa

---

[76] HE 20/2013 vp, s. 79.

olisi otettava huomioon ulkoisen tapahtuman *säännönmukaisuus* ja *ennalta-arvattavuus*.[77] Sähköverkkoja hallinnoiviin järjestelmiin kohdistettu kyberhyökkäys voitaisiin mahdollisesti lukea tällaiseksi muuksi odotettavissa olevaksi ulkoiseksi häiriöksi, sillä kyberhyökkäyksiä on Euroopassakin säännönmukaisesti tapahtunut ja ne on yleisesti tunnustettu merkittäväksi uhaksi myös sähköverkkojen toiminnalle. Kyberhyökkäys voitaisiin myös mahdollisesti katsoa kolmannen kohdan mukaiseksi *normaaliolojen häiriötilanteeksi*, jonka varalta sähköverkon olisi toimittava mahdollisimman luotettavasti. Myöskään 19 §:ssä tai sen soveltamista täsmentävässä hallituksen esityksessä ei kuitenkaan oteta nimenomaisesti kantaa tietojärjestelmien ja -verkkojen kyberturvallisuuteen.

Voitaisiinko siis edellä esitettyjä säännöksiä tulkita niin, että niistä pystyttäisiin johtamaan sähköverkonhaltijoihin kohdistuvia, konkreettisia kyberturvallisuusvelvoitteita? Tilanteissa, joissa säännöksen soveltuvuus tiettyyn oikeustosiseikastoon ei käy selvästi ilmi pykälän tekstistä, voidaan mahdollisesti käyttää *oikeudellista analogiaa*, joka tarkoittaa säännöksen soveltamisalan laventamista. Säännöksen analoginen soveltaminen voidaan katsoa oikeudellisesti hyväksyttäväksi tilanteissa, joissa oikeustosiseikasto on riittävän samankaltainen kuin tiukasti sanamuodon mukaisessa soveltamistilanteessa.[78] Sähkömarkkinalain kontekstissa voitaisiin siis pohtia, voidaanko 19 §:n velvoitteita soveltaa analogisesti myös sähköverkonhaltijoiden hallinnoimiin tietojärjestelmiin- ja verkkoihin.

Asiaa arvioitaessa voidaan kuitenkin melko nopeasti tulla siihen tulokseen, että oikeudellinen analogia ei tässä tapauksessa voi tulla kyseeseen, vaan sen sijaan tilanteeseen on sovellettava *oikeudellista distinktiota*, eli tietyn oikeustosiseikaston rajaamista sovellusalan ulkopuolelle.[79] Tätä voidaan perustella sillä, että edellä mainittu analoginen laventaminen menisi tässä tapauksessa eittämättä liian kauas 19 §:n ytimestä. Säännöksissä ei mainita erikseen mitään tietojärjestelmistä ja -verkoista, saati niiden kyberturvallisuudesta. Lisäksi, kun säännöksiä tarkastellaan laajemmin koko sähkömarkkinalain kontekstissa, huomataan, että ne ovat luonteeltaan yleisiä ja vaativat täsmennystä muista lainkohdista tai kokonaan muusta lainsäädännöstä. Kun muualta löytyvät säännökset tai lain esityötkään eivät viittaa millään tavalla siihen, että kyseisillä pykälillä olisi tarkoitettu luoda verkonhaltijoille varsinaisia

---

[77] HE 20/2013 vp, s. 79.

[78] Siltala 2010, s. 233.

[79] Siltala 2010, s. 233.

kyberturvallisuusvelvoitteita, voidaan perustellusti argumentoida, ettei tässä tapauksessa ole oikeudellisia perusteita lain analogiseen soveltamiseen. Liian lavea soveltaminen olisi myös vastoin *oikeusvarmuuden periaatetta*.

Myös NIS-direktiivin implementointiin liittyvä hallituksen esitys tukee käsitystä, jonka mukaan edellä esitellystä 19 §:stä ei voida johtaa verkonhaltijoihin kohdistuvia kyberturvallisuusvelvoitteita. Hallituksen esityksessä todetaan, että vaikka sähkömarkkinalaista on ennen NIS-direktiivin implementointiakin löytynyt joitakin riskienhallintavelvoitteita, *näitä ei ole voitu katsoa direktiivin edellyttämiksi, viestintäverkkojen ja tietojärjestelmien turvallisuuteen tähtääviksi velvoitteiksi*. Tästä syystä kyseisessä hallituksen esityksessä ehdotettiinkin sähkömarkkinalakiin uusia nimenomaisia pykäliä, joilla sähköverkonhaltijat velvoitettaisiin huolehtimaan myös viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta, sekä ilmoittamaan merkittävistä järjestelmien tietoturvallisuuteen liittyvistä häiriöistä Energiavirastolle.[80] Näitä säännöksiä käsitellään seuraavaksi.

3.2.5 Sähkömarkkinalain kyberturvallisuusvelvoitteet

Sähkömarkkinalain 29 a ja 28 pykälät ovat verkonhaltijoiden kyberturvallisuusvelvoitteiden osalta kaikista merkittävimmät kansalliset säännökset. NIS-direktiivi on pantu sähköverkkojen osalta täytäntöön juuri 29 a §:llä ja se kuuluu seuraavanlaisesti:

> *Verkonhaltijan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen*
>
> Verkonhaltijan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.
>
> Verkonhaltijan on ilmoitettava viipymättä Energiavirastolle sellaisesta sen käyttämiin viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena sähkönjakelu voi keskeytyä jakeluverkossa merkittävässä laajuudessa.
>
> Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Energiavirasto voi velvoittaa palvelun tarjoajan tiedottamaan yleisölle asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.

---

[80] HE 192/2017 vp., s. 51.

> Energiaviraston on arvioitava, koskeeko 2 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille jäsenvaltioille.
>
> Energiavirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö *(pitäisi ilmeisesti viitata 2 momenttiin)* on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

Pykälän ensimmäisessä momentissa tuodaan tiiviisti ilmi velvoite huolehtia viestintäverkkojen ja tietojärjestelmien kyberturvallisuudesta. Tätä hyvin pelkistettyä ilmausta täsmennetään lain esitöissä muun muassa toteamalla, että riskienhallinnalla tarkoitettaisiin *asianmukaisia organisatorisia ja teknisiä toimenpiteitä*, joilla varmistettaisiin viestintäverkkojen ja tietojärjestelmien kyky suojautua tietyllä varmuudella toimilta, jotka vaarantavat järjestelmissä olevien tietojen tai palveluiden saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Lisäksi mainitaan, että riskienhallinnan tulisi sisältää *asianmukaiset toimenpiteet, joilla ehkäistään ja minimoidaan* järjestelmien tietoturvallisuuteen liittyvien häiriöiden vaikutus palveluiden jatkuvuuteen.

Hallituksen esityksessä mainitaan myös esimerkinomaisina riskienhallintatoimenpiteinä *turvallisuussuunnitelmien laatiminen ja testaaminen*, *järjestelmien auditoiminen*, *tiedon suojaus- ja salaustuotteiden käyttö*, sekä *tiettyjen tunnettujen tietoturvastandardien, kuten ISO/IEC 27001:2013- standardin, noudattaminen.*[81] Hallituksen esityksessä viitataan siis pitkälti NIS-direktiivin 14 artiklan ilmauksiin ja yleisiin tietoturvallisuuden määritelmiin. Verrattuna NIS-direktiiviin, lisää täsmennystä toimenpiteiden käytännön toteutukseen saadaan oikeastaan vain hallituksen esityksessä luetelluista toimenpide-esimerkeistä.

Ensimmäisen momentin kohdalla on huomionarvoista, että itse pykäläteksti on hyvin pelkistetty, jopa verrattuna sen pohjana olevaan NIS-direktiivin 14 artiklaan. Lisäksi, kuten jo luvussa 3.2.2 todettiin, direktiivin potentiaalisesti merkittävä vaatimus *uusimman tekniikan* huomioimisesta on jätetty kokonaan pois 29 a §:stä sekä lain esitöistä. Näiltä osin direktiivin implementoinnin onnistuminen voidaan perustellusti kyseenalaistaa. Pelkkää sähkömarkkinalakia lukemalla ei näet voi saada selvää kuvaa siitä, mihin konkreettisiin toimiin sähköverkonhaltijoiden tulisi ryhtyä kyberturvallisuudesta huolehtimiseksi. Vaikuttaa siltä, että velvoitteiden ymmärtämiseksi on välttämätöntä tutustua hallituksen esitykseen sekä

[81] HE 192/2017 vp., s. 77.

NIS-direktiiviin, ja pykälää on pyrittävä tulkitsemaan *EU-oikeuden yhdenmukaisen tulkinnan periaatteen* mukaisesti yhdessä NIS-direktiivin kanssa.

Sähkömarkkinalain 29 a §:n velvoittavuutta ja käytännön toimivuutta voidaan kuitenkin kritisoida myös siksi, että edes hallituksen esitystä lukemalla ja yhdenmukaisen tulkinnan periaatetta noudattamalla, pykälä ei tunnu asettava sähköverkonhaltijoille konkreettisia riskienhallintavelvoitteita. Ensinnäkin, kuten luvussa 3.2.2 todettiin, myöskään NIS-direktiivissä ei merkittävästi täsmennetä siinä esitettyjä riskienhallintavelvoitteita. Mahdollisesti ainoa direktiivistä johdettava lisätulkinta voisi liittyä uusimman tekniikan vaatimukseen, mutta kun tämäkään ilmaus ei saa koko direktiiviä tarkasteltaessa sen konkreettisempaa merkitystä, ei sähkömarkkinalain tulkitsemisella yhdenmukaisesti NIS-direktiivin kanssa saavuteta juurikaan lisää selvyyttä asiaan.

Tähän väliin on todettava, että kuten luvussa 3.2.3 tuotiin esille, tuore NIS2 -direktiivi voi jo tässä vaiheessa saada kansallisen sääntelyn tulkintaa ohjaavaa vaikutusta. Uudessa direktiivissä kyberturvallisuusriskien hallintatoimenpiteitä on täsmennetty huomattavasti alkuperäiseen NIS-direktiiviin verrattuna. Näin ollen, mikäli sähkömarkkinalain 29 a §:n mukaisia toimenpidevaatimuksia puitaisiin esimerkiksi oikeudessa, voisi tuomioistuin saada huomattavaa tulkinnallista lisäapua tuoreesta NIS2 -direktiivistä. Koska tässä tutkielmassa keskitytään kuitenkin alkuperäiseen NIS-direktiiviin, ei näitä mahdollisia tulkintavaikutuksia lähdetä sen enempää arvioimaan. Luvussa 5.2 avataan kuitenkin vielä erikseen NIS2 -direktiivin sisältöä.

Toiseksi, lain esitöissä todetaan selväsanaisesti, että *laissa ei määriteltäisi tarkemmin, miten riskienhallinnasta olisi huolehdittava, vaan tältä osin toimijalla (tässä tapauksessa sähköverkonhaltijalla) olisi mahdollisuus valita liiketoimintaansa, järjestelmiinsä ja muuhun riskienhallintaansa parhaiten sopivat menetelmät tietoturvariskien hallitsemiseksi.*[82] Lisäksi lain esitöissä todetaan, että NIS-direktiivin myötä tulleilla uusilla velvoitteilla *ei olisi merkittäviä taloudellisia vaikutuksia palveluntarjoajille*.[83]

Vaikuttaakin siltä, että sähkömarkkinalain 29 a § ei tällä hetkellä edellytä sähköverkonhaltijoilta mitään konkreettisia toimenpiteitä kyberturvallisuudesta

[82] HE 192/2017 vp., s. 59.

[83] HE 192/2017 vp., s. 59.

huolehtimiseksi. Kun vielä lainsäätäjä on arvioinut, että pykälän mukaisilla toimenpiteillä ei pitäisi olla mitään taloudellisia vaikutuksia toimijoille, voidaan perustellusti argumentoida, ettei säännös ole tarpeeksi täsmällinen, eikä siitä voida johtaa tehokkaita kyberturvallisuusvelvoitteita.

Sähkömarkkinalain 29 a §:n toisessa momentissa määrätään, että verkonhaltijan on ilmoitettava viipymättä Energiavirastolle *merkittävästä* tietoturvallisuuden häiriöstä, jonka seurauksena sähkönjakelu voi keskeytyä jakeluverkossa merkittävässä laajuudessa. Lain esitöissä mainitaan, että tietoturvallisuuteen liittyvällä häiriöllä tarkoitettaisiin mitä tahansa tapahtumaa, joka tosiasiallisesti vaikuttaisi haitallisesti kyseessä olevien järjestelmien turvallisuuteen. Poikkeaman merkittävyyden määrittämiseksi olisi myös otettava huomioon erityisesti niiden käyttäjien lukumäärä, joihin häiriö vaikuttaa, häiriön kesto sekä maantieteellinen levinneisyys.[84] Säännös vastaa siis pitkälti NIS-direktiivin 14 artiklan kolmatta kohtaa.

Energiavirasto on antanut vuonna 2018 ohjeen[85], jolla täsmennetään ilmoitusmenettelyä sekä ilmoituskynnystä. Ohjeen mukaan Energiaviraston olisi saatava ilmoituksessa *riittävät tiedot häiriön luonteesta*, *vakavuudesta* sekä *vaikutuksista sähkönjakeluun*. Ohjeessa lisäksi täsmennetään ilmoituksen sisältöä, erittelemällä tarkemmin asioita, joita ilmoituksesta tulisi vähintäänkin löytyä. Ohjeessa esitetään myös tiukennus pykälätekstin mukaiseen ilmoituskynnykseen, ja siinä pyydetään verkonhaltijoita ilmoittamaan *kaikista* viestintäverkkoihin ja tietojärjestelmiin kohdistuvista tietoturvallisuuteen liittyvistä häiriöistä, joiden seurauksena *on aiheutunut tai olisi voinut aiheutua* sähkönjakelun keskeytys. Kyseinen ohje ja siinä ilmenevä tiukennus eivät kuitenkaan ole tarkalleen ottaen oikeudellisesti sitovia. Tätä viranomaisen antaman ohjeen velvoittavuuteen liittyvää problematiikkaa avataan jäljempänä 28 §:n ja siihen liittyvän toisen Energiaviraston antaman ohjeen käsittelyn yhteydessä.

---

[84] HE 192/2017 vp., s. 78.

[85] Energiaviraston ohje tietoturvallisuuteen liittyvän häiriön ilmoittamisesta (1914/402/2018).

3.2.6 Sähkömarkkinalain edellyttämä varautumissuunnittelu ja Energiaviraston tarkentavat ohjeet

Sähkömarkkinalain 28 §:ssä säädetään verkonhaltijan varautumissuunnittelusta seuraavaa:

> Verkonhaltijan on asianmukaisella suunnittelulla varauduttava sähköverkkoonsa kohdistuviin normaaliolojen häiriötilanteisiin, sähköjärjestelmässä ilmenevien sähkönsaannin häiriöiden edellyttämien säännöstelytoimenpiteiden täytäntöönpanoon ja valmiuslaissa tarkoitettuihin poikkeusoloihin. Verkonhaltijan on laadittava varautumissuunnitelma sekä osallistuttava tarpeellisessa laajuudessa huoltovarmuuden turvaamiseen tähtäävään valmiussuunnitteluun. Varautumissuunnitelma on päivitettävä vähintään kerran kolmessa vuodessa ja silloin, kun olosuhteissa tapahtuu merkittäviä muutoksia.
>
> …
>
> Varautumissuunnitelma ja siihen tehtävät muutokset on toimitettava Energiavirastolle. Energiavirastolla on oikeus kuuden kuukauden kuluessa varautumissuunnitelman vastaanottamisesta vaatia verkonhaltijaa tekemään siihen muutoksia, jos se ei täytä säädettyjä vaatimuksia.

Kyseinen säännös luo sähköverkonhaltijoille velvollisuuden varautua häiriöihin myös *kirjallisen varautumissuunnitelman* muodossa. Nimenomaan *kyberturvallisuuden häiriöihin* varautumiseen otetaan kuitenkin kantaa vasta Energiaviraston antamassa ohjeessa[86], jossa täsmennetään 28 §:n määräyksiä. Ohjeen alussa todetaan, että koska tietoturvariskien hallinta liittyy olennaisesti verkonhaltijan varautumissuunnitteluun, on varautumissuunnitelmassa tuotava esille muun ohella myös *tietoturvariskienhallinnan perusperiaatteet ja toimintamallit.* Samassa kohtaa todetaan myös, että kuten lain esitöissäkin velvoitetaan, tietoturvariskienhallinta on tehtävä dokumentoidusti ja dokumentointi voidaan ottaa osaksi 28 §:n mukaista varautumissuunnitelmaa.[87] Näin ollen verkonhaltija voi siis osoittaa sähkömarkkinalain 29 a §:n mukaisten riskienhallintavelvoitteiden noudattamisen liittämällä niihin liittyvän selvityksen 28 §:n mukaiseen varautumissuunnitelmaan.

Kyseinen Energiaviraston ohje, tai tarkemmin ottaen sen liitteenä oleva *Sähköverkonhaltijan varautumissuunnitelman mallipohja,* on tämän tutkielman kannalta erittäin huomionarvoinen, sillä vasta kyseisessä mallipohjassa varsinaisesti konkretisoidaan 29 a §:n mukaisia

---

[86] Energiaviraston ohjeistus sähköverkonhaltijoiden varautumis- ja valmiussuunnittelusta 2022 (232/040002/2022).

[87] Energiavirasto 2022, s. 1.

riskienhallintavelvoitteita. Ohjeen mukaan mallipohjan käyttäminen ei ole pakollista, mutta siinäkin tilanteessa, että verkonhaltija päättäisi laatia varautumissuunnitelmansa vapaamuotoisesti, olisi suunnitelmaan sisällytettävä vähintäänkin mallipohjasta löytyvät asiat. Näin ollen mallipohjan voidaan katsoa olevan käytännössä osa virallista ohjetta.[88]

Viestintäverkkojen ja tietojärjestelmien riskien hallinta on mallipohjassa eriytetty omaksi luvukseen, millä on haluttu korostaa kyberturvallisuuden kasvavaa merkitystä myös sähköverkonhaltijoiden toiminnassa. Kyseisessä luvussa eritellään hyvin seikkaperäisesti kyberturvallisuuden eri osa-alueita sekä käytännön toimia, joihin sähköverkonhaltijoiden tulisi ryhtyä kyberturvallisuudesta huolehtimiseksi.

Mallipohjassa käsitellään muun muassa 1) *kyberturvallisuuden hallintaa*, jonka osalta pyydetään tarkkaa kuvausta yrityksen kyberturvallisuuspolitiikasta-, strategiasta ja -ohjelmasta. Näissä tulisi kuvata esimerkiksi kyberturvallisuuden valvontakäytänteitä, tietoturvallisuuden hoitamiseen liittyviä tehtäviä ja vastuuhenkilöitä, yrityksen sidosryhmien perehdyttämistä kyberturvallisuusasioihin, asiakirjojen ja dokumenttien tietoturvallista hallintatapaa, henkilöstön osaamista ja koulutusta, sekä sisäisten että ulkoisten auditointien tekemistä. Lisäksi samassa kohdassa pyydetään yksilöimään yrityksen käytössä olevat *standardit*, *kybermaturiteetin mittaustyökalut* sekä *tietoturvan hallintajärjestelmät*.[89]

Mallipohjassa pyydetään myös kuvailemaan hyvin yksityiskohtaisesti yrityksen 2) *kyberturvallisuusarkkitehtuuria*, jonka osia ovat muun muassa verkkojen segmentointi, ylläpitoratkaisut, salausmenetelmät sekä jäljityslokit. Yrityksiä pyydetään lisäksi kuvailemaan omaksumiaan 3) *identiteetin- ja pääsynhallintakäytänteitä*, 4) *kriittisten tieto- ja tietoliikennejärjestelmien jatkuvuudenhallintaa*, *sähkönsyötön varmistamista* ja *muuta suojaamista sekä varajärjestelmiä*. Lisäksi pyydetään yksityiskohtaisia kuvauksia 5) *vakavien tietoturvahaavoittuvuuksien ja häiriöiden tunnistamisesta ja niistä toipumisesta.*[90]

Kaiken kaikkiaan mallipohja antaa sähköverkonhaltijayrityksille hyvin kattavan ja yksityiskohtaisen ohjeistuksen huomioitavista kyberturvallisuuden osa-alueista sekä konkreettisista toimenpiteistä kyberturvallisuudesta huolehtimiseksi. Tässä vaiheessa herää

---

[88] Energiavirasto 2022, s. 4.

[89] Energiavirasto 2022, Sähköverkonhaltijan varautumissuunnitelman mallipohja (232/040002/2022), s. 18–28.

[90] Energiavirasto 2022, Sähköverkonhaltijan varautumissuunnitelman mallipohja (232/040002/2022), s. 18–28.

kuitenkin luonnollisesti kysymys siitä, mikä on tämän, Energiaviraston antaman ohjeen liitteenä olevan mallipohjan velvoittavuus, eli kuinka vahvasta oikeuslähteestä on juridisesti kysymys?

Suomessa viranomainen voi antaa lakia täsmentäviä *määräyksiä*, vain jos sille on laissa nimenomaisesti annettu tällainen toimivaltuus.[91] Kyseinen sääntö voidaan johtaa perustuslain 80 §:stä. Ensinnäkään, sähkömarkkinalaissa ei ole annettu Energiavirastolle valtuutta antaa tarkempia määräyksiä niistä toimista, joihin sähköverkonhaltijoiden tulisi ryhtyä tietojärjestelmiensä ja -verkkojensa suojelemiseksi. Lain 29 a §:n viidennen momentin valtuutuskin koskee ainoastaan määräyksiä, jotka täsmentävät verkonhaltijoiden *ilmoitusvelvollisuutta*.

Toiseksi, viranomaisen antama *määräys* on myös syytä erottaa käsitteellisesti viranomaisen antamasta *ohjeesta*, jollainen tässäkin käsiteltävä Energiaviraston asiakirja tarkalleen ottaen on. Oikeusministeriön tuottamassa *Lainkirjoittajan oppaassa* todetaan ohjeen oikeudellisesta luonteesta seuraavaa:

> ”Ohje” ei ole oikeussääntö eikä myöskään oikeudellisesti sitova. Ohje voi olla esimerkiksi neuvo, käyttöohje tai jokin suositus. Viranomainen voi laissa säädetyn tehtävänsä alalla antaa ohjeita ilman erityistä valtuutusta.[92]

Sama näkemys on vahvistettu myös oikeuskirjallisuudessa, jossa ohjeellisen tai suositusluonteisen viranomaissäännöksen on katsottu tarkoittavan viranomaisten antamia erilaisia lainsoveltamisohjeita ja -määräyksiä, *joilta puuttuu oikeudellinen sitovuus*.[93]

Edellä esitelty *Energiaviraston ohjeistus sähköverkonhaltijoiden varautumis- ja valmiussuunnittelusta 2022* ei siis perustu missään lakipykälässä annettuun valtuutukseen, eikä se ole myöskään *ohjeena* oikeudellisesti sitova. Voisiko Energiaviraston ohje saada kuitenkin välillistä velvoittavuutta esimerkiksi sitä kautta, että sähkömarkkinalain 29 a ja 28 §:iä tulkittaisiin yhdenmukaisesti sen kanssa?

---

[91] Mäenpää 2018, s. 210.

[92] Oikeusministeriö 2022.

[93] Siltala 2010, s. 189; Mäenpää 2018, s. 213.

Kysymys on juridisesti mielenkiintoinen ja vaatii asian tarkastelemista myös perustuslain tasolla. Perustuslain 107 §:n mukaan asetuksen tai muun lakia alemman asteisen säädöksen säännöstä ei saa soveltaa tuomioistuimessa tai muussa viranomaisessa, mikäli kyseinen säännös on ristiriidassa perustuslain tai muun lain kanssa. Toisin sanoen, lakia alempi säädös väistyy, mikäli se on ristiriidassa kyseisen lain kanssa. Jotta Energiaviraston ohjeelle voitaisiin antaa edes sähkömarkkinalain tulkintaa ohjaavaa merkitystä, ohje ei näin ollen saisi olla ristiriidassa sähkömarkkinalain kanssa. Kuten seuraavassa kappaleessa tarkemmin selitetään, tällainen ristiriita vaikuttaisi kuitenkin olevan olemassa.

Energiaviraston ohjeessa todetaan, että se perustuu sähkömarkkinalain 29 a ja 28 §:iin. Kyseiset pykälät ovat luonteeltaan niin yleisiä, ettei niiden tekstistä voida sinänsä löytää mitään, mikä olisi ristiriidassa pykälien soveltamista täsmentämään tarkoitetun ohjeen kanssa. Tässä vaiheessa kuvaan astuu kuitenkin jälleen kerran aiemmin mainittu lain esitöiden tulkintakannanotto, jonka mukaan sähköverkonhaltijalle on jätetty harkintavalta sen suhteen, millaisin *konkreettisin toimenpitein* se huolehtii riskienhallinnan toteuttamisesta.[94] Tässä lainsäätäjä esittää selkeästi historiallisen tarkoituksensa ja tulkinnan sen puolesta, että sähkömarkkinalain tarkoituksena ei ole loppujen lopuksi velvoittaa mihinkään konkreettisiin toimenpiteisiin kyberturvallisuudesta huolehtimiseksi. Näin ollen voitaisiin ajatella, että perustuslain 107 §:n hengessä, Energiaviraston antama ohje on tietyllä tavalla ristiriidassa sähkömarkkinalain kanssa, eikä se voisi senkään vuoksi vaikuttaa sähkömarkkinalain tulkintaan, saatikka saada muuta oikeudellista velvoittavuutta.

3.2.7 Yhteenveto kyberturvallisuuden velvoitesääntelystä

Kuten edellisistä luvuista on varmasti käynyt ilmi, sähköverkonhaltijoihin kohdistuvat kyberturvallisuusvelvoitteet ovat kaikkea muuta kuin yksinkertaisia ja selkeitä. Tästä syystä seuraavaksi on tarkoitus kerrata edellä esitelty lainopillinen analyysi ja esittää mahdollisimman tiivisti ja ymmärrettävästi nykyinen oikeustila, niin EU-oikeudellisella kuin kansallisellakin tasolla.

Suomessa ei ole yhtä kyberturvallisuuden yleislakia, vaan sääntely on jakaantunut kunkin toimialan omaan erityislainsäädäntöön. Sähköverkkojen osalta relevantteja säädöksiä ovat Euroopan unionin tasolla *EU:n verkko ja tietoturvadirektiivi (NIS-direktiivi)*, (nykyisin myös

[94] HE 192/2017 vp., s. 59.

NIS2 -direktiivi), sekä kansallisella tasolla *sähkömarkkinalaki*. Lisäksi huomionarvoisia ovat *Energiaviraston ohjeistus sähköverkonhaltijoiden varautumis- ja valmiussuunnittelusta 2022* mallipohjineen, sekä *Energiaviraston ohje tietoturvallisuuteen liittyvän häiriön ilmoittamisesta*.

NIS-direktiivin merkittävimmät säännökset löytyvät sen 14 artiklasta. Artiklan mukaiset velvoitteet kohdistuvat juridisesti jäsenvaltioihin, ja niiden mukaan jäsenvaltioiden tulee varmistaa, että kriittiset toimijat toteuttavat asianmukaiset ja oikeasuhteiset tekniset ja organisatoriset toimenpiteet kyberturvallisuudesta huolehtimiseksi. Lisäksi jäsenvaltioiden tulee varmistaa, että toimijat ilmoittavat merkittävistä kyberturvallisuuden poikkeamista valvoville viranomaisille.

Vaikka direktiivillä on selvästi pyritty korkeatasoiseen kyberturvallisuuteen koko unionin alueella, sen säännöksistä ei voida johtaa mitään konkreettisia riskinhallintavelvoitteita. Käytännössä vain ilmoitusvelvollisuus vaikuttaa sen verran selkeältä, että direktiivillä voitaisiin nykyisellään saavuttaa tähän liittyvät tavoitteet.

Sähköverkonhaltijoiden osalta NIS-direktiivin velvoitteet on pantu täytäntöön sähkömarkkinalain muutoksilla. Merkittävimmät sähkömarkkinalain säännökset ovat 28 § (verkonhaltijan varautumissuunnittelu) sekä 29 a § (verkonhaltijan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen). Valitettavasti direktiivin implementointi vaikuttaa kuitenkin puutteelliselta, eikä lainsäätäjä ole onnistunut konkretisoimaan kyberturvallisuusriskien hallintaan liittyviä velvoitteita myöskään sähkömarkkinalaissa. Lainvalmisteluasiakirjoista käy myös selvästi ilmi, että nykyisillä pykälillä ei ole edes tarkoitettu antaa tarkkoja määräyksiä vaadittavista toimista, vaan toimijoille on jätetty valta päättää toimenpiteiden käytännön toteutuksesta. Ainoat yksityiskohtaisesti kuvaillut riskienhallintatoimenpiteet löytyvät Energiaviraston antamasta ohjeesta, mutta se ei ole oikeuslähteenä sitova.

Kaiken kaikkiaan vallitseva oikeustila vaikuttaa siltä, että lainsäädännöstämme ei löydy konkreettisia, sähköverkonhaltijoita velvoittavia kyberturvallisuusriskien hallintaan liittyviä velvoitteita. Riittävä kyberuhkiin varautuminen vaikuttaa jääneen toimijoiden oman aktiivisuuden varaan.

Nykyisen sääntelyn puutteellisuus onkin tunnistettu EU-tasolla, mistä todisteena on juuri julkaistu NIS2 -direktiivi. Direktiivin mahdollisesta tulkintaa ohjaavasta vaikutuksesta mainittiin edellä, mutta varsinaisesti uudistuksen vaikutukset tulevat näkymään vasta seuraavan parin vuoden aikana, kun direktiivi pannaan kansallisesti täytäntöön, ja mitä todennäköisimmin myös sähkömarkkinalakia muutetaan sen mukaiseksi. Asiaan palataan vielä luvussa 5.2.

3.3 Sähköverkkojen kyberturvallisuuden viranomais-, valvonta- ja sanktiosääntely

3.3.1 Toimivaltaiset viranomaiset

Kyberturvallisuuden velvoitesääntelyn lisäksi on hyvä tarkastella myös velvoitteiden noudattamiseen liittyvää viranomais- valvonta- ja sanktiosääntelyä. Seuraavissa luvuissa esitellään viranomaiset, jotka vastaavat sähköverkonhaltijoiden toiminnan valvonnasta, sekä näiden viranomaisten toimivaltuudet. Tarkastelussa keskitytään toimivaltuussääntelyyn, joka koskee velvoitteiden noudattamisen valvontaa sekä noudattamatta jättämisestä seuraavia täytäntöönpanotoimia ja sanktioita.

Tarkastelu on rajattu koskemaan kansallisia viranomaisia, sillä nämä tahot vastaavat käytännössä sähköverkonhaltijoiden toiminnan valvonnasta myös EU-tasoisten säännösten osalta. Tutkimus keskittyy lisäksi vain *hallinnolliseen sääntelyyn*, eikä asiaa lähestytä esimerkiksi sopimusoikeudellisesta tai rikosoikeudellisesta näkökulmasta. Tämä tarkoittaa muun muassa sitä, että luvussa 3.3.3 käsitellään yksinomaan hallinnollisia sanktioita, kuten valtiolle maksettavia, velvoitteiden noudattamatta jättämisestä seuraavia *seuraamusmaksuja*. Tutkimuksessa ei käsitellä esimerkiksi vahingonkorvauksia, joita sähköverkonhaltija saattaisi joutua maksamaan, mikäli sen laiminlyönneistä olisi aiheutunut haittaa muille yksityisille toimijoille. Käsittelyyn ei oteta myöskään ongelmatilanteista mahdollisesti seuraavia rikosoikeudellisia sanktioita tai oikeusprosesseja.

Sähkömarkkinalain 106 §:n mukaan *Energiavirasto* valvoo sähkömarkkinalain ja sen nojalla annettujen säännösten noudattamista, ja tästä valonnasta säädetään tarkemmin *sähkö- ja maakaasumarkkinoiden valvonnasta annetussa laissa (590/2013)*. Lisäksi NIS-direktiivin 8 artiklassa säädetään jäsenvaltioiden velvollisuudesta nimetä *kansalliset toimivaltaiset viranomaiset* valvomaan direktiivin velvoitteiden noudattamista. Energiavirasto toimii

energia-alalla kansallisena toimivaltaisena viranomaisena, eli se vastaa muun ohella myös NIS-direktiivin mukaisten kyberturvallisuusvelvoitteiden valvonnasta.

NIS direktiivissä säädetään myös jäsenvaltioiden velvollisuudesta nimetä yksi viranomainen *keskitetyksi kansalliseksi yhteyspisteeksi*, jonka tehtävänä on vastata kyberturvallisuuteen liittyvästä yhteistyöstä muiden EU-maiden kanssa. Lisäksi NIS-direktiivissä velvoitetaan jäsenvaltiot nimeämään yksi tai useampi *tietoturvaloukkauksiin reagoiva ja niitä tutkiva yksikkö (CSIRT-toimija)*, jonka tehtävänä on ehkäistä, havaita ja lieventää verkko- ja tietojärjestelmien poikkeamia kansallisella tasolla, sekä tehdä näihin liittyvää yhteistyötä muiden EU-maiden vastaavien viranomaisten kanssa. Sähköisen viestinnän palveluista annetun lain 308 §:n mukaan Suomessa *Liikenne- ja viestintävirasto (Traficom)* toimii kumpanakin NIS-direktiivin edellyttämänä viranomaisena, ja käytännössä tästä toiminnasta vastaa Traficomin alainen *Kyberturvallisuuskeskus*.

3.3.2 Kyberturvallisuusvelvoitteiden valvontaan liittyvä sääntely

NIS-direktiivin 15 artiklassa määrätään direktiivin täytäntöönpanosta ja sen mukaisten velvoitteiden valvonnasta seuraavaa:

> 1. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on tarvittavat valtuudet ja keinot arvioida, noudattavatko keskeisten palvelujen tarjoajat 14 artiklan mukaisia velvollisuuksiaan, sekä tämän vaikutuksia verkko- ja tietojärjestelmien turvallisuuteen.
>
> 2. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on valtuudet ja keinot pyytää keskeisten palvelujen tarjoajia
>
> a) antamaan tiedot, jotka tarvitaan niiden verkko- ja tietojärjestelmien turvallisuuden arvioimiseksi, mukaan lukien todennettavassa muodossa olevat turvallisuusohjeet;
>
> b) esittämään näyttöä turvallisuusohjeiden tosiasiallisesta täytäntöönpanosta, kuten toimivaltaisen viranomaisen tai pätevän tarkastajan suorittaman turvallisuustarkastuksen tulokset, ja viimeksi mainitussa tapauksessa antamaan turvallisuustarkastuksen tulokset, mukaan lukien niitä tukeva näyttö, toimivaltaisen viranomaisen käyttöön.
>
> …
>
> 3. Toimivaltainen viranomainen voi 2 kohdassa tarkoitettujen tietojen tai turvallisuustarkastusten tulosten arvioinnin jälkeen antaa keskeisten palvelujen tarjoajille sitovia ohjeita havaittujen puutteiden korjaamiseksi.

Kyseisessä artiklassa jäsenvaltiot velvoitetaan siis varmistamaan, että toimivaltaisilla viranomaisilla on tosiasialliset keinot valvoa direktiivin noudattamista, sekä puuttua keskeisten palvelujen tarjoajien toimintaan, mikäli velvoitteet on laiminlyöty. Direktiivin mukaan esimerkiksi Energiaviraston tulisi pystyä valvomaan sähköverkonhaltijoiden toimintaa ja antaa näille sitovia ohjeita korjaustoimenpiteistä, mikäli verkonhaltijat eivät ole noudattaneet kyberturvallisuusvelvoitteitaan.

NIS-direktiivin kansallisen täytäntöönpanon yhteydessä, toimivaltaisille viranomaisille *ei annettu* uusia, nimenomaan direktiivin mukaisten kyberturvallisuusvelvoitteiden valvontaan liittyviä toimivaltuuksia. Tämä on todettu muun muassa oikeusministeriön vuonna 2019 tekemässä selvityksessä *Viranomaisten toimivaltuudet häiriötilanteissa*.[95] Sen sijaan on katsottu, että nämä direktiivin edellyttämät toimivaltuudet tulee johtaa jo aiemmin sektorikohtaisesta lainsäädännöstä löytyneistä säännöksistä.

Sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain (jäljempänä *valvontalaki*) 9 §:ssä säädetään Energiaviraston toimivallasta valvonta-asioissa seuraavaa:

> Jos joku rikkoo tai laiminlyö 2 §:ssä tarkoitetussa kansallisessa tai Euroopan unionin lainsäädännössä säädettyjä velvoitteitaan, Energiamarkkinaviraston on velvoitettava hänet korjaamaan rikkomuksensa tai laiminlyöntinsä. Päätöksessä voidaan määrätä, millä tavoin rikkomus tai laiminlyönti tulee korjata.

Tähän väliin täsmennyksenä, että viittauksella 2 §:ään tarkoitetaan muun muassa sähkömarkkinalakia, ja Energiamarkkinaviraston tilalla on nykyisin Energiavirasto. Saman lain 30 §:ssä säädetään lisäksi Energiaviraston tiedonsaanti- ja tarkastusoikeudesta seuraavaa:

> Valvottavaa toimintaa harjoittavan elinkeinonharjoittajan (…) on annettava Energiavirastolle tässä laissa tarkoitettujen valvontatehtävien hoitamiseksi tarpeelliset tiedot ja asiakirjat. Tämän lisäksi Energiavirastolle on annettava muiden tässä laissa tarkoitettujen tehtävien hoitamiseksi tai kansainvälisten sopimusvelvoitteiden täyttämiseksi tarpeellisia tilasto- ja muita tietoja.
>
> Energiaviraston asianomaisella virkamiehellä on oikeus tässä laissa tarkoitetun valvontatehtävän toteuttamiseksi (…) toimittaa tarkastus valvottavaa toimintaa harjoittavan elinkeinonharjoittajan hallinnassa olevissa tiloissa. Tarkastusta ei kuitenkaan saa suorittaa pysyväisluonteiseen asumiseen käytetyssä tilassa. Tarkastusta toimittavalle virkamiehelle ja Energiaviraston valtuuttamalle muulle henkilölle on järjestettävä pääsy elinkeinonharjoittajan hallinnassa oleviin tiloihin sekä niihin sähkö- tai maakaasulaitteisiin ja -laitteistoihin, joilla voi olla

[95] Oikeusministeriö 2019, s. 30.

> merkitystä tässä laissa tarkoitettujen valvontatehtävien hoitamisessa. Tarkastusta toimittavalla virkamiehellä on oikeus tutkia elinkeinonharjoittajan asiakirjat ja data, joilla voi olla merkitystä tässä laissa tarkoitettujen valvontatehtävien hoitamisessa, ja ottaa niistä jäljennöksiä maksutta. Energiavirasto voi tarkastuksessa käyttää apunaan muita valtuuttamiaan henkilöitä.

Kyseisillä pykälillä Energiavirastolle annetaan siis yleinen toimivalta puuttua muun muassa sähkömarkkinalain vastaiseen toimintaan, velvoittaa toimija korjaamaan rikkomuksensa tai laiminlyöntinsä, sekä tarkemmat valtuudet valvontaa varten tarvittavien asiakirjojen vastaanottamisesta ja tarkastusten suorittamisesta. Säännöksiä ei juuri täsmennetä lain esitöissä.

Valvontalaissa ei ole säännöksiä nimenomaan kyberturvallisuusvelvoitteiden valvonnasta. Tässä vaiheessa onkin siis pohdittava, antavatko valvontalain 9 ja 30 §:t Energiavirastolle tarvittavat valtuudet ja keinot myös kyberturvallisuusvelvoitteiden valvomiseen. Vaikkei valvontalaissa nimenomaisesti viitatakkaan kybervelvoitteiden valvomiseen, voitaisiin kyseisten pykälien ajatella antavan tähän sinänsä riittävät toimivaltuudet, sillä säännöksissä kuitenkin viitataan yleisesti sähkömarkkinalain vastaiseen toimintaan. Samaa mieltä on ollut myös lainsäätäjä, ja NIS-direktiivin implementointiin liittyvässä hallituksen esityksessä todetaan seuraavaa: ”Viranomaisella on toimivalta valvoa tietoturvallisuuteen liittyvien velvoitteiden noudattamista ja velvoittaa korjaamaan lain vastainen toiminta, vain mikäli toimivallasta on säädetty. *Toimivallasta voidaan säätää yleisesti (esimerkiksi Energiavirasto)* tai erityisesti (tietyssä pykälässä säädettyjä velvoitteita valvoo tietty viranomainen).”[96]

Nykyistä oikeustilaa on kuitenkin myös kritisoitu. Oikeusministeriö on tarkastellut selvityksessään *Viranomaisten toimivaltuudet häiriötilanteissa* eri alojen valvovien viranomaisten toimivaltuuksia puuttua NIS-direktiivin mukaisten velvoitteiden vastaiseen toimintaan. Selvityksessä ei tarkastella nimenomaisesti Energiaviraston toimivaltaa, mutta siinä todetaan yleisesti, että muilla toimivaltaisilla viranomaisilla, kuin Traficomilla televiestintäalan valvonnassa, oikeustila vaikuttaa olevan tällä hetkellä epäselvä.[97] Väitettä avataan esimerkillä Traficomin toimivallasta rautatietoimijoiden valvonnassa (tilanne ja

[96] HE 192/2017 vp., s. 56.

[97] Oikeusministeriö 2019, s. 31.

siihen liittyvä sääntely vastaavat käytännössä hyvin pitkälti Energiaviraston asemaa sähköverkonhaltijoiden toiminnan valvojana).

Oikeusministeriö toteaa selvityksessään, että *on vähintäänkin epäselvää, voisivatko rautatielaista löytyvät yleiset, valvontaan liittyvät toimivaltuudet, oikeuttaa liikenne- ja viestintäviraston antamaan rautatiealan toimijoille tarkempia, sitovia määräyksiä kyberturvallisuustoimista*. Asiaa perustellaan muun muassa sillä, että julkisen vallan käytön tulisi perustua lakiin, ja että laissa olisi säädettävä täsmällisesti niistä toimivaltuuksista ja niistä seuraamuksista, joita lain rikkomisesta seuraa.[98]

Myös liikenne- ja viestintäministeriö on kritisoinut nykyistä oikeustilaa ja todennut raportissaan *Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla*, että vaikka viranomaisen valvontatoimivaltuudet olisivatkin periaatteessa kunnossa, ongelmaksi voi käytännössä muodostua se, että monilla kriittisillä toimialoilla ei ole yksinkertaisesti riittävän konkreettisia kyberturvallisuusvelvoitteita, joita valvoa.[99] Raportissa tuodaan esille eri alojen valvovien viranomaisten, sekä tietoturva-arviointeja tekevien toimijoiden mielipiteet siitä, että *konkreettisemmat vaatimukset tehostaisivat valvontaa, sillä niiden täyttyminen olisi helpompi todentaa, kuin laissa olevien, hyvin yleistasoisesti muotoiltujen velvoitteiden toteutuminen*.[100]

Toisin sanoen ongelmana vaikuttaa olevan se, että kun lainsäädännössä ei ole alun perinkään määritelty riittävän selkeästi vaadittavia kyberturvallisuustoimia, ei valvova viranomainen voi todellisuudessa todeta valvottavan tahon toimia riittämättömiksi. Kuten aiemmissa luvuissa on tuotu ilmi, sähköverkonhaltijoihin kohdistuvat kyberturvallisuusvelvoitteet vaikuttavat tällä hetkellä puutteellisilta, joten ongelma tuntuu koskettavan myös Energiaviraston harjoittamaa valvontaa.

Valvontatoimivaltuuksiin liittyvät epäselvyydet onkin tunnistettu myös EU-tasolla, ja uuteen NIS2 -direktiivin on otettu entistä täsmällisempiä valvontasäännöksiä. Näitä muutoksia käsitellään tarkemmin vielä luvussa 5.2.

---

[98] Oikeusministeriö 2019, s. 31; Mäenpää 2018, s. 144.

[99] Liikenne- ja viestintäministeriö 2021, s. 32.

[100] Liikenne- ja viestintäministeriö 2021, s. 28–29.

3.3.3 Sanktiosääntely ja viranomaisten nykyinen resurssitilanne

Tärkeä osa viranomaisvalvontaa ovat velvoitteiden noudattamatta jättämisestä seuraavat sanktiot. NIS-direktiivin 21 artiklassa säädetään direktiivin velvoitteiden rikkomisen seuraamuksista seuraavaa:

> Jäsenvaltioiden on säädettävä tämän direktiivin nojalla annettujen kansallisten säännösten rikkomiseen sovellettavista seuraamuksista ja toteutettava kaikki tarvittavat toimenpiteet sen varmistamiseksi, että ne pannaan täytäntöön. Säädettyjen seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia.

Artikla on sisällöltään melko selkeä, ja se velvoittaa jäsenvaltiot varmistamaan, että niiden lainsäädännöstä löytyy riittävän tehokkaat, oikeasuhteiset ja varoittavat seuraamukset direktiivin mukaisten velvoitteiden noudattamatta jättämisestä.

Direktiivin täytäntöönpanon yhteydessä valvontalakiin ei otettu uusia säännöksiä kyberturvallisuusvelvoitteiden rikkomisesta seuraavista sanktioista. Asiaa ei myöskään käsitellä lain esitöissä, ja lainsäätäjä onkin ilmeisesti katsonut, että valvontalaista jo löytyvät seuraamussäännökset riittäisivät vastaamaan NIS-direktiivin 21 artiklan vaatimuksiin.

Valvontalain 16 §:n mukaan sähköverkonhaltijalle voidaan määrätä *seuraamusmaksu*, jos tämä tahallaan tai huolimattomuudesta rikkoo tiettyjä, pykälässä erikseen mainittuja säännöksiä. Näitä erikseen mainittuja säännöksiä ovat muun muassa monet sähkömarkkinalain pykälät, mutta on huomionarvoista, että säännöksestä *ei löydy viittausta* verkonhaltijan varautumissuunnittelua tai kyberturvallisuusvelvoitteita koskeviin sähkömarkkinalain 28 ja 29 a §:iin. Näin ollen seuraamusmaksu ei vaikuta tällä hetkellä koskevan ollenkaan kyberturvallisuusvelvoitteiden rikkomista.

Asia varmistuu valvontalain esitöissä, joissa todetaan, että seuraamusmaksu voidaan tuomita *vain pykälässä yksilöityjä säännöksiä* rikkovalle elinkeinonharjoittajalle.[101] Tämä tarkoittaa sitä, että valvontalain 16 §:ssä esitetty säännösten lista on tyhjentävä, eikä näin ollen Energiavirastolla ole tällä hetkellä minkäänlaista lakiin perustuvaa toimivaltaa määrätä sähköverkonhaltijoille seuraamusmaksuja, mikäli nämä rikkovat kyberturvallisuusvelvoitteitaan. On huomionarvoista, että esimerkiksi Iso-Britannian sekä Puolan kansallisessa lainsäädännössä on määritelty hyvinkin yksityiskohtaisesti

[101] HE 20/2013 vp., s. 166.

hallinnollisista sakoista, jotka koskettavat *kaikkia* NIS-direktiivin soveltamisalaan kuuluvia toimijoita.[102] Näin ollen voidaan ajatella, että toisin kuin monet muut jäsenmaat, Suomi on ainakin sähköverkkojen osalta epäonnistunut *tehokkaiden*, *oikeasuhteisten* ja *varoittavien* seuraamusten implementoimisessa.

Valvontalain 23 §:ssä säädetään sähkö- ja maakaasuverkkoluvan peruuttamisesta seuraavaa:

> Energiavirasto voi peruuttaa sähköverkkoluvan:
>
> 1) jos luvanhaltija lopettaa verkkotoiminnan;
>
> 2) jos luvanhaltija ei enää täytä luvan myöntämisen edellytyksiä;
>
> 3) jos luvanhaltija *toistuvasti ja oleellisesti rikkoo* lupaehtoja, *sähkömarkkinalakia* (…) eikä luvanhaltijalle etukäteen annettu varoitus luvan peruuttamisesta ole johtanut toiminnassa esiintyneiden puutteiden korjaamiseen.

Tässä yhteydessä huomionarvoinen on kolmas kohta, jonka mukaan Energiavirasto voi peruuttaa sähköverkkoluvan, mikäli luvanhaltija on toistuvasti ja oleellisesti rikkonut sähkömarkkinalakia varoituksista huolimatta. Säännöstä ei juuri täsmennetä lain esitöissä. Voitaisiin siis ajatella, että mikäli sähköverkonhaltija rikkoo vakavasti ja varoituksista huolimatta sähkömarkkinalain mukaisia kyberturvallisuusvelvoitteitaan, Energiavirastolla voisi olla toimivalta peruuttaa sähköverkonhaltijan toimilupa.

Kyseinen toimenpide olisi kuitenkin eittämättä hyvin ankara ja pitkälle menevä, ja olisikin hyvin epätodennäköistä, että kyberturvallisuusvelvoitteiden noudattamatta jättäminen johtaisi tosimaailmassa sähköverkkoluvan peruuttamiseen. Mikäli nimittäin verkonhaltija olisi vaarassa menettää toimilupansa tällaisesta syystä, olisi se hyvin todennäköisesti motivoitunut korjaamaan laiminlyöntinsä jo varoituksen jälkeen. Lisäksi kuten edellä todettiin, Energiavirastolla vaikuttaisi olevan tällä hetkellä lähtökohtaisestikin vaikeuksia valvoa kyberturvallisuusvelvoitteiden noudattamista puutteellisesta velvoitesääntelystä johtuen, mistä syystä 23 §:n aktualisoituminen nykytilanteessa olisi hyvin epätodennäköistä.

---

[102] Calder 2018, s. 22–23; Chałubińska-Jentkiewicz – Radoniewicz – Zieliński 2022, s. 365–378.

Kun vielä kyseistä säännöstä ei ehkä voitaisi pitää NIS-direktiivin 21 artiklan vaatimalla tavalla *oikeasuhteisena*, voidaan perustellusti argumentoida, että myöskään valvontalain 23 §:n mukainen sähköverkkoluvan menettäminen ei näyttäisi soveltuvan (ainakaan käytännössä elämässä) kyberturvallisuusvelvoitteiden rikkomisesta seuraavaksi sanktioksi. Tähän väliin on tosin huomionarvoista todeta, että NIS2 -direktiivissä edellytetään, että kyberturvallisuusvelvoitteiden rikkomistilanteissa toimivaltaisilla viranomaisilla tulisi olla oikeus *keskeyttää väliaikaisesti sertifiointi tai lupa, joka koskee toimijan palveluja*. Tältä osin myös valvontalain 23 §:ään saattaa tulla muutoksia lähivuosina.

Valvontalain 31 §:ssä säädetään Energiaviraston oikeudesta asettaa *uhkasakko* tekemänsä päätöksen tai asettamansa velvoitteen noudattamisen tehosteeksi. Uhkasakon voitaisiin ajatella olevan toteutuessaan tehokas kannustin myös kyberturvallisuustoimissa ilmenevien puutteiden korjaamiseen, mutta tässäkin tapauksessa säännöksen käytännön toimivuus voidaan jälleen kyseenalaistaa. Jos näet Energiavirasto ei käytännössä kykene osoittamaan kyberturvallisuusvelvoitteiden noudattamatta jättämistä, ei se myöskään voi asettaa uhkasakkoa puutteiden korjaamisen kannusteeksi.

Kaiken kaikkiaan vaikuttaa siis siltä, että NIS-direktiivin vaatimuksia tehokkaista, oikeasuhteisista ja varoittavista seuraamuksista ei ole implementoitu kunnolla kansalliseen lainsäädäntöön, mikä entisestään aiheuttaa kannustinongelmia sähköverkonhaltijoiden kyberturvallisuusvelvoitteiden noudattamiseen. Ongelma onkin tunnistettu EU-tasolla, ja NIS2 -direktiivin myötä myös seuraamussäännöksiä on huomattavasti täsmennetty ja kiristetty. Asiaa avataan vielä tarkemmin luvussa 5.2.

Puutteellisen sääntelyn lisäksi, viranomaisten mahdollisuuksia valvoa kyberturvallisuusvelvoitteiden noudattamista rajoittaa nykyisin myös akuutti *resurssivaje*. Liikenne- ja viestintäministeriön raportissa Tietoturvan ja tietosuojan parantamisesta yhteiskunnan kriittisillä toimialoilla todetaan useassa kohtaa, ettei valvovilla viranomaisilla ole tällä hetkellä riittäviä tosiasiallisia resursseja valvontaan ja toimivaltuuksien hyödyntämiseen.[103]

Eri alojen valvontaviranomaisten lisäksi, myös Kyberturvallisuuskeskuksen resursseissa olisi kehitettävää, sillä ainakaan raportin julkaisun aikaisten tietojen valossa

[103] Liikenne- ja viestintäministeriö 2021, s. 32 ja 51.

Kyberturvallisuuskeskus ei ole pystynyt tarjoamaan riittäviä tukipalveluita kaikille yhteiskunnan kriittisille toimialoille.[104] Raportin laatineen työryhmän arvion mukaan, kriittisten toimialojen valvoville viranomaisille tarvittaisiin kaikkinensa 109 henkilötyövuotta lisää, jotta valvonta, ohjaus ja neuvonta saataisiin vaadittavalle tasolle.[105] Myös toimivaltaiset viranomaiset itse, kuten Energiavirasto, ovat peräänkuuluttaneet riittävien resurssien ja virkamiesten osaamisen välttämättömyyttä.[106]

Viranomaisten resursseihin ja toimintakykyyn vaikuttavana tekijänä on myös tunnistettu tietoturvaosaajien puute työmarkkinoilla. Tämä vaikeuttaa viranomaisten rekrytointeja, sillä harvoista osaajista joudutaan kilpailemaan yksityisen sektorin ja muiden viranomaisten kanssa.[107]

Nykyinen resurssitilanne vaikuttaa olevan myös suoraan NIS-direktiivin vastainen. Direktiivin 8 ja 9 artikloissa, sekä johdanto-osan 31 kappaleessa todetaan selvästi, että toimivaltaisilla viranomaisilla, CSIRT-toimijalla sekä keskitetyllä yhteyspisteellä tulisi olla *riittävät tekniset ja taloudelliset resurssit sekä henkilöresurssit,* jotta ne voisivat toteuttaa niille osoitetut tehtävät tehokkaasti ja tuloksekkaasti ja siten saavuttaa direktiivin tavoitteet.

[104] Liikenne- ja viestintäministeriö 2021, s. 35.

[105] Liikenne- ja viestintäministeriö 2021, s. 57.

[106] Energiavirasto 2021, s. 1.

[107] Liikenne- ja viestintäministeriö 2021, s. 32.

4 Muiden kriittisten toimialojen kyberturvallisuussääntely

4.1 Digitaalisen infrastruktuurin kyberturvallisuussääntely

4.1.1 Digitaalisen infrastruktuurin kyberturvallisuuden velvoitesääntely

Seuraavissa luvuissa tarkastellaan valikoivasti muiden kriittisten toimialojen kyberturvallisuussääntelyä ja verrataan tätä sähköverkkojen sääntelyyn. Käsiteltäviksi toimialoiksi on valittu *digitaalinen infrastruktuuri*, *finanssimarkkinat* sekä *terveydenhuoltoala*. Kyseiset toimialat on valittu vertailukohdiksi siitä syystä, että niiden kyberturvallisuussääntely vaikuttaa olevan tällä hetkellä yksityiskohtaisempaa ja velvoittavampaa kuin sähköverkkojen vastaava sääntely. Kattavimmin käsitellään digitaalista infrastruktuuria, sillä se on näistä toimialoista luonteeltaan ja ominaisuuksilta lähinnä sähköverkkoja.

Muiden kriittisten toimialojen, kuten esimerkiksi maakaasuverkkojen, vesihuollon sekä liikenteen kyberturvallisuusääntely on lain tasolla melko samanlaista kuin sähköverkoilla. Vertailu näiden alojen välillä ei siis olisi kovin mielenkiintoista, mistä syystä ne on rajattu tämän tutkielman ulkopuolelle.

Samaan tapaan kuin sähköverkkojen osalta, myös seuraavissa luvuissa käsitellään sekä velvoitesääntelyä että viranomaisvalvontaan ja sanktioihin liittyvää sääntelyä. Käsittelyssä keskitytään kansalliseen sääntelyyn. NIS-direktiiviä sovelletaan yleisesti myös finanssimarkkinoiden sekä terveydenhuoltoalan toimijoihin, joten lukujen 3.2.1, 3.2.2 ja 3.2.3 lainopillinen analyysi kuvaa hyvin myös näiden alojen EU-tasoisia kyberturvallisuuden vähimmäisvaatimuksia. Digitaalisen infrastruktuurin alalla esimerkiksi *teleyritykset* eivät kuulu NIS-direktiivin soveltamisalaan, mutta niin sanotussa *teledirektiivissä*[108] on asetettu teleyrityksille vähintäänkin yhtä kattavat velvoitteet huolehtia kyberturvallisuudestaan. Lisähuomiona voidaan tässä kohtaa todeta, että myös teleyritykset tulevat siirtymään NIS2 -direktiivin soveltamisalan piiriin sitten, kun direktiivin implementointiaika on kulunut loppuun. Edellä mainituista syistä EU-sääntelyä ei enää erikseen käsitellä seuraavissa luvuissa.

---

[108] Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/1972, annettu 11 päivänä joulukuuta 2018, eurooppalaisesta sähköisen viestinnän säännöstöstä (teledirektiivi).

Samoin kuin sähkömarkkinoilla, myös digitaalisen infrastruktuurin alalla toimii lukuisia yrityksiä erilaisissa rooleissa. Alan toimijoita ovat muun muassa *teleyritykset*, *nimipalvelujen tarjoajat*, *verkossa toimivat markkinapaikat ja hakukoneet* sekä *pilvipalvelujen tarjoajat.*

Vaikka kaikilla digitaaliseen infrastruktuuriin lukeutuvilla toimijoilla on oma merkityksensä, kaikista huomattavimpia alan toimijoita ovat kuitenkin teleyritykset.[109] Ne määritellään sähköisen viestinnän palveluista annetun lain 3 §:n 27 kohdassa *yrityksiksi, jotka tarjoavat verkkopalvelua tai viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille, eli harjoittavat yleistä teletoimintaa*. Teleyrityksen määritelmä on laaja, mutta ehkä merkittävimpiä määritelmän alaan kuuluvia toimijoita ovat niin sanotut *perinteiset teleyritykset*, jotka tarjoavat esimerkiksi puhelinpalveluita ja internetyhteyksiä hallitsemiensa viestintäverkkojen välityksellä.[110]

Nämä yritykset ovat merkittäviä juuri niiden omistaman ja hallitseman viestintäverkkoinfrastruktuurin takia, sillä kyseinen infrastruktuuri on elintärkeää niin toimijoiden itsensä, kuin myös muiden alan yritysten toiminnan kannalta. Tarkemmin ottaen toimivat ja turvalliset viestintäverkot mahdollistavat loppupeleissä kaiken internetiä hyödyntävän liiketoiminnan, ja tästä syystä myös tässä luvussa keskitytään digitaalisen infrastruktuurin osalta juuri teleyrityksiin ja niitä koskevaan kyberturvallisuussääntelyyn.

Teleyritysten kyberturvallisuusvelvoitteista säädetään pääosin *sähköisen viestinnän palveluista annetussa laissa (SVPL).* Yksi merkittävimmistä säännöksistä on SVPL:n 243 §, jossa säädetään muun ohella teleyrityksien hallinnoimien viestintäverkkojen ja -palveluiden kyberturvallisuusvaatimuksista valikoiden seuraavaa:

> Yleiset viestintäverkot ja -palvelut sekä niihin liitettävät viestintäverkot ja -palvelut on suunniteltava, rakennettava ja ylläpidettävä siten, että:
>
> 1) sähköinen viestintä on tekniseltä laadultaan hyvää ja tietoturvallista,
>
> 2) ne kestävät normaalit odotettavissa olevat ilmastolliset, mekaaniset, sähkömagneettiset ja muut ulkoiset häiriöt sekä tietoturvauhat,

---

[109] HE 192/2017 vp., s. 50.

[110] Liikenne- ja viestintävirasto 2022. Sääntelyn kohteet. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/saantelyn-kohteet. (Luettu 28.11.2022).

> 4) niihin kohdistuvat merkittävät tietoturvaloukkaukset ja -uhat sekä niiden toimivuutta merkittävästi häiritsevät viat ja häiriöt voidaan havaita,
>
> 7) kenenkään tietosuoja, tietoturva tai muut oikeudet eivät vaarannu,
>
> 9) ne eivät aiheuta kohtuuttomia sähkömagneettisia tai muita häiriöitä taikka tietoturvauhkia,
>
> 14) ne toimivat mahdollisimman luotettavasti myös valmiuslaissa (1552/2011) tarkoitetuissa poikkeusoloissa ja normaaliolojen häiriötilanteissa,
>
> Edellä 1 momentin 1–4, 10, 11 ja 14 kohdassa tarkoitetut laatuvaatimukset on suhteutettava viestintäverkkojen ja -palvelujen käyttäjämäärään, maantieteelliseen alueeseen, jota ne palvelevat, sekä niiden merkitykseen käyttäjille.
>
> Toimenpiteet, joilla huolehditaan 1 momentin 1, 2, 4, 7 ja 9 kohdassa tarkoitetusta tietoturvasta, tarkoittavat toimia toiminnan turvallisuuden, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden sekä tietoaineistoturvallisuuden varmistamiseksi. Toimenpiteet on suhteutettava uhan vakavuuteen, toimenpiteistä aiheutuviin kustannuksiin sekä käytettävissä oleviin teknisiin mahdollisuuksiin torjua uhka.

Säännöstä voidaan verrata sähkömarkkinalain 19 §:ään, jossa säädetään sähköverkkojen laatuvaatimuksista. Siinä missä sähkömarkkinalain pykälässä ei kuitenkaan edes mainita tietoturvallisuutta, SVPL:n 243 §:ssä asiaa käsitellään monestakin eri näkökulmasta.

Säännöksen mukaan sähköisen viestinnän on oltava yleisesti tekniseltä laadultaan hyvää ja tietoturvallista, ja viestintäverkkojen sekä -palveluiden on kestettävä normaalit odotettavissa olevat tietoturvauhat. Uhkien määritelmää tarkennetaan lain esitöissä niin, että kyseinen pykälä edellyttää suojautumaan *tietoturvauhilta, jotka ovat teleyrityksen normaalilla asiantuntemuksella ja ammattitaidolla ennakoitavissa.*[111]

Merkittävät tietoturvaloukkaukset ja -uhat on myös kyettävä *havaitsemaan*, mikä tarkoittaa lain esitöiden mukaan sitä, että häiriöiden olisi oltava ennalta tunnistettavissa, jotta niiden vuoksi voitaisiin ryhtyä tarvittaviin toimenpiteisiin. Esitöiden mukaan säännöksen tarkoituksena on asettaa viestintäverkon ja -palvelun tarjoajalle velvollisuus seurata ja valvoa sen hallinnassa olevia verkkoja ja palveluita, esimerkiksi seuraamalla viestiliikenteen kulkua ja liikennettä haittaavia tekijöitä, sekä asettamalla automaattisia hälytyksiä tietyille tekijöille,

---

[111] HE 221/2013 vp., s. 181.

joiden avulla voidaan tunnistaa tietoturvauhkia. Tällaisten havaintojen perusteella voitaisiin tarvittaessa ryhtyä muualla laissa määriteltyihin toimiin häiriön korjaamiseksi, kuten esimerkiksi haittaa aiheuttavan verkonosan tai palvelun irrottamiseen yleisestä viestintäverkosta.[112]

Pykälän ensimmäisen momentin 7 kohdan mukaan kenenkään tietosuoja tai tietoturva eivät saisi vaarantua teleyrityksen harjoittaman toiminnan vuoksi, millä tarkoitetaan käytännössä sitä, että teleyritysten hallinnoimien verkkojen ja palveluiden tulee olla niin turvallisia, etteivät ne aiheuta tietoturvaongelmia verkkojen ja palveluiden *käyttäjille*. Yhdeksäs kohta tarkoittaa puolestaan sitä, että viestintäverkot ja -palvelut eivät saa aiheuttaa tietoturvauhkia myöskään *muille verkoille tai palveluille*.[113] Pykälän toisessa ja kolmannessa momentissa tarkennetaan ja osittain rajataan ensimmäisen momentin vaatimuksia.

Säännöksen velvoitteet vaikuttavat kaiken kaikkiaan selvästi kattavammilta, kuin sähkömarkkinalaista löytyvät kyberturvallisuusvelvoitteet. Siinä missä esimerkiksi sähkömarkkinalain 29 a §:ssä puhutaan vain yleisesti viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta, SVPL:n 243 §:ssä esitetään monenlaisia vaatimuksia tietoturvasta huolehtimiseksi. Tietoturvaa käsitellään useista eri näkökulmasta, minkä lisäksi myös SVPL:n esitöiden pykäläkohtaisissa perusteluissa säännösten sisältöä tarkennetaan perusteellisemmin, kuin sähkömarkkinalain vastaavassa lainvalmistelumateriaalissa. Kuitenkin myös SVPL:n 243 § jää sellaisenaan hieman yleiselle tasolle, eikä pelkästään sen perusteella voida esittää kovin konkreettisia kyberturvallisuusvaatimuksia.

Sähköisen viestinnän palveluista annetusta laista löytyykin lisää tarkentavia säännöksi, muun muassa *toimista, joihin teleyrityksillä on oikeus ryhtyä tietoturvasta huolehtimiseksi*. Esimerkiksi lain 272 §:ssä säädetään teleyritysten oikeudesta valvoa, rajoittaa ja tarvittaessa myös estää haitallista viestintää niiden hallitsemissa verkoissa. Pykälän mukaan toimijoilla on myös oikeus poistaa tietoturvaa vaarantavat haitalliset tietokoneohjelmat tai ryhtyä muihin vastaavanlaisiin teknisiin toimenpiteisiin tietoturvasta huolehtimiseksi. Viestien valvonnan ja käsittelemisen tulee olla turvallisuuden kannalta välttämätöntä ja teknisten toimenpiteiden lähtökohtaisesti *automaattisia*. Kuitenkin, mikäli on ilmeistä, että tarkastelun kohteena oleva viesti sisältää haitallisen tietokoneohjelman, eikä ohjelmaa kyetä automaattisilla toimilla

[112] HE 221/2013 vp., s. 181–182.

[113] HE 221/2013 vp., s. 182.

poistamaan, on teleyrityksellä oikeus käsitellä viestin sisältöä myös *manuaalisesti*. Kaikkien käsittelytoimien tulee olla oikein mitoitettuja ja huolellisesti toteutettuja, eikä niillä saa rajoittaa sananvapautta, luottamuksellisen viestin suojaa tai yksityisyyden suojaa enempää kuin on välttämätöntä. Mikä merkittävintä, säännöksessä annetaan myös Liikenne- ja viestintävirastolle valtuus antaa *tarkempia määräyksiä* pykälän mukaisten toimenpiteiden teknisestä toteuttamisesta.

Lisää kyberturvallisuuteen liittyviä säännöksiä löytyy SVPL:n 273 §:stä, jossa säädetään *teleyrityksen velvollisuudesta korjata sen hallitseman viestintäverkon, viestintäpalvelun tai laitteen aiheuttamat merkittävät häiriöt*. Pykälän mukaan toimijan on välittömästi ryhdyttävä toimenpiteisiin tilanteen korjaamiseksi ja tarvittaessa irrotettava viestintäverkko, viestintäpalvelu tai laite yleisestä viestintäverkosta. Toimenpiteet on jälleen kerran toteutettava huolellisesti ja ne on mitoitettava suhteessa torjuttavan häiriön vakavuuteen. Säännöksessä annetaan myös Liikenne- ja viestintävirastolle toimivalta tarvittaessa päättää pykälässä kuvatuista korjaustoimenpiteistä ja verkon, palvelun tai laitteen irrottamisesta.

Sähköisen viestinnän palveluista annetun lain 244 a §:n mukaan viestintäverkkolaitetta ei saa käyttää yleisen viestintäverkon kriittisissä osissa, jos on painavia perusteita epäillä, että laitteen käyttäminen vaarantaisi kansallista turvallisuutta tai maanpuolustusta siten, että käytöllä mahdollistettaisiin ulkomainen tiedustelutoiminta tai toiminta, jolla häirittäisiin, lamautettaisiin tai muuten vahingollisella tavalla vaikutettaisiin Suomen tärkeisiin etuihin, yhteiskunnan perustoimintoihin tai kansanvaltaiseen yhteiskuntajärjestykseen. Mikäli tällainen haitallinen verkkolaite havaitaan teleyrityksen hallinnoimassa verkossa, Liikenne- ja viestintävirastolla on oikeus velvoittaa teleyritys poistamaan haittaa aiheuttava laite.

Säännös on siinä mielessä huomionarvoinen, että siinä korostetaan nimenomaan kansallisesta turvallisuudesta ja maanpuolustuksesta huolehtimista, ja vaadittavien toimenpiteiden motiiveina esitetään ulkomaisen tiedustelutoiminnan ja häirinnän estäminen. Esimerkiksi sähkömarkkinalaissa ei esitetä sähköverkkojen suojelulle mitään tällaisia, kansallista turvallisuutta tai yhteiskunnan toimivuutta korostavia perusteluja, vaikka ne voisivat eittämättä toimia kannustimina myös sähköverkkoja koskevan kyberturvallisuussääntelyn yhteydessä.

Lisäksi SVPL:n 274 §:ssä säädetään teleyrityksen velvollisuudesta ilmoittaa asiakkailleen sen palveluihin kohdistuvista merkittävistä tietoturvaloukkauksista, ja 275 §:ssä puolestaan velvollisuudesta tehdä samanlainen ilmoitus Liikenne- ja viestintävirastolle.

Sähköisen viestinnän palveluista annetusta laista löytyy myös yleisiä säännöksiä teleyritysten velvollisuudesta varautua normaaliolojen häiriötilanteisiin ja poikkeusoloihin, sekä tähän liittyvästä varautumissuunnittelusta. Nämä säännökset ovat sisällöllisesti hyvin samankaltaisia, kuin sähkömarkkinalaista löytyvät varautumisvelvoitteet.

Kaiken kaikkiaan edellä esitellyt SVPL:n mukaiset säännökset kyberturvallisuudesta huolehtimiseksi ovat selvästi yksityiskohtaisempia, kuin sähkömarkkinalain vastaavat säännökset. Kuitenkin se, mikä varsinaisesti tekee teleyrityksiä koskevasta sääntelystä merkittävästi konkreettisempaa ja velvoittavampaa verrattuna sähköverkkojen sääntelyyn, on Liikenne- ja viestintävirastolle annettu *määräyksenantovaltuus*.

Sähköisen viestinnän palveluista annetun lain 244 §:n mukaan Liikenne- ja viestintävirasto voi nimittäin antaa tarkempia *määräyksiä* viestintäverkkojen ja palveluiden laadusta ja tietoturvallisuudesta. Nämä määräykset voivat koskea esimerkiksi 1) viestintäverkon ja siihen kuuluvan laitetilan sähköistä ja fyysistä suojaamista, 2) suorituskykyä, tietoturvallisuutta ja häiriöttömyyttä sekä niiden ylläpitoa, seurantaa ja verkonhallintaa, 3) menettelyä vika- tai häiriötilanteissa, 4) toimia tietoturvallisuuden ja toimintavarmuuden ylläpitämiseksi, sekä 5) muita näihin verrattavia teknisiä vaatimuksia. Lisäksi joissakin yksittäisissä SVPL:n pykälissä annetaan Liikenne- ja viestintävirastolle valtuus antaa kyseisiä säännöksiä tarkentavia määräyksiä. Kuten tutkielmassa on aiemmin todettu, nämä SVPL:n nojalla annettavat määräykset ovat *oikeudellisesti sitovia.*

Liikenne- ja viestintävirasto on käyttänyt valtuuttaan ahkerasti, ja sen on antanut lakia täydentäviä määräyksiä muun muassa *teletoiminnan tietoturvasta*, *teletoiminnan häiriötilanteista*, *viestintäverkon kriittisistä osista* sekä *viestintäverkkojen ja -palveluiden turvaamisesta normaaliolojen häiriötilanteissa ja poikkeusoloissa*.

Esimerkiksi *Liikenne- ja viestintäviraston määräyksessä 67 teletoiminnan tietoturvasta*[114], sekä *määräystä tarkentavassa perustelu- ja soveltamisasiakirjassa*[115] esitetään hyvin yksityiskohtaisia kyberturvallisuusvaatimuksia. Vaatimukset koskevat esimerkiksi tietoturvallisuuden eri osa-alueiden huomioimista ja dokumentointia, riskien tunnistamista ja hallintaa, hallintaverkon suojaamista, verkon rajapintojen erityisiä vaatimuksia, internetyhteyspalvelujen erityisiä vaatimuksia, sähköpostipalvelujen erityisiä vaatimuksia sekä erilaisia tiedottamisvelvoitteita. Laajuudessaan ja yksityiskohtaisuudessaan kyseinen määräys on verrattavissa luvussa 3.2.6 esiteltyyn Energiaviraston ohjeeseen[116], mutta siinä missä Energiaviraston asiakirja on vain suositusluontoinen *ohje*, Liikenne- ja viestintäviraston määräys on edellä mainituin tavoin oikeudellisesti sitova. Näin ollen teleyritykset ovat tällä hetkellä aidosti velvoitettuja kattaviin ja konkreettisiin toimiin kyberturvallisuudesta huolehtimiseksi.

Telealaa koskevia määräyksiä ollaan myös uudistamassa, millä pyritään vastaamaan viime vuosina tapahtuneeseen teknologiseen kehitykseen. Esimerkiksi verkon monimuotoistuminen, uusien rajapintojen avaaminen, virtualisointi, 5G-teknologia sekä pilvipalvelut ovat esimerkkejä kehityksestä, jonka vuoksi Liikenne- ja viestintäviraston Määräystä 67 ollaan parhaillaan päivittämistä.[117]Digitaalisen infrastruktuurin alalla nykyinen oikeustila vaikuttaakin olevan selvästi parempi kuin sähkömarkkinoilla.

Luvun loppuun voitaisiin nostaa vielä yksi mielenkiintoinen velvoitesäännös digitaalisen infrastruktuurin alalta, joka koskee muun muassa *vahvojen sähköisten tunnistuspalveluiden tarjoajia*. Näitä palveluja ovat esimerkiksi pankkien verkkopankkitunnuksia hyödyntävät tunnistuspalvelut sekä teleyritysten mobiilivarmenteet. Kyseisten palvelujen laatuvaatimuksista säädetään *vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (617/2009)*. Lain 29 §:n mukaan tunnistuspalvelun tarjoajan on määräajoin teetettävä palvelulleen erillisen arviointielimen suorittama *auditointi*, jonka avulla on tarkoitus selvittää, täyttääkö kyseinen tunnistuspalvelu vaaditut tietoturvaa,

---

[114] Liikenne- ja viestintävirasto, Määräys 67 teletoiminnan tietoturvasta, 67 A/2015 M.

[115] Liikenne- ja viestintävirasto, Määräyksen 67 perustelut ja soveltaminen, MPS 67, 4.3.2015.

[116] Energiavirasto, Energiaviraston ohjeistus sähköverkonhaltijoiden varautumis- ja valmiussuunnittelusta 2022 (232/040002/2022).

[117] Liikenne- ja viestintävirasto, Määräyshankepäätös, Määräyksen 67 päivittäminen, 10.6.2022, s. 1.

tietosuojaa ja muuta luotettavuutta koskevat vaatimukset. Pykälän mukaan Liikenne- ja viestintävirasto voi myös antaa tarkempia määräyksiä auditoinnissa käytettävistä arviointiperusteista.

Auditoinneilla tarkoitetaan tässä yhteydessä tietynlaisia *tietoturva-tarkastuksia*, joita voidaan kohdistaa organisaation hallitsemiin tietojärjestelmiin tai sen toimintaan yleisemmin. Tällä hetkellä tietoturvaa koskevia auditointeja tekevät Suomessa Kyberturvallisuuskeskus, erikseen hyväksytyt arviointilaitokset (KPMG ja Nixu), eräät tietoturvayritykset sekä organisaatioiden sisäiset riippumattomat toimijat.[118]

Vaatimus järjestelmien tietoturva-auditoinneista on katsottu hyväksi keinoksi parantaa toimijoiden kyberturvallisuutta. Auditointien hyvänä puolena on nähty muun muassa se, että toimijat saavat niiden perusteella konkreettista tietoa järjestelmiensä kyberturvallisuuden tasosta, sekä ohjeita puutteiden korjaamiseen. Auditointiraporteista voi myös olla huomattava apu viranomaisvalvonnassa, sillä ne antavat valvovalle viranomaiselle selkeän kuvan valvottavan toimijan kyberturvallisuuden tasosta.[119]

On huomionarvoista, että tällä hetkellä sähköverkonhaltijoihin ei kohdistu lainsäädännössä minkäänlaisia auditointivelvoitteita, vaikka käytäntö voisi olla perusteltu myös tällä alalla. Valtioneuvosto onkin periaatepäätöksessään ehdottanut, että kaikille kriittisille toimialoille säädettäisiin velvoite säännöllisten tietoturva-auditointien teettämiseen.[120]

4.1.2 Digitaalisen infrastruktuurin viranomais-, valvonta- ja sanktiosääntely

Varsinaisten velvoitesäännösten lisäksi on syytä tarkastella myös digitaalisen infrastruktuurin kyberturvallisuuteen liittyvää *viranomais-, valvonta- ja sanktiosääntelyä*. Liikenne- ja viestintävirasto toimii alan yleisenä valvontaviranomaisena, ja näin ollen se valvoo myös teleyritysten kyberturvallisuusvelvoitteiden noudattamista.

Viraston *yleisestä valvontatehtävästä* säädetään sähköisen viestinnän palveluista annetun lain 303 §:ssä. Tätä täydennetään 304 §:llä, jonka mukaan Liikenne- ja viestintäviraston *erityisinä tehtävinä* ovat muun muassa 1) edistää sähköisen viestinnän toimivuutta, häiriöttömyyttä ja

---

[118] Liikenne- ja viestintäministeriö 2021, s. 43.

[119] Liikenne- ja viestintäministeriö 2021, s. 41.

[120] Valtioneuvosto 2021, s. 7.

turvallisuutta, 2) osallistua valmiussuunnitteluun sekä valvoa ja kehittää alan teknistä varautumista poikkeusoloihin, sekä 3) selvittää verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin sekä tietojärjestelmiin kohdistuvia tietoturvaloukkauksia ja niiden uhkia.

Lain 315 §:ssä puolestaan säädetään Liikenne- ja viestintäviraston *yleisestä oikeudesta saada valvontatehtäviensä suorittamiseksi tarvittavat tiedot* niiltä, joiden oikeuksista ja velvollisuuksista laissa säädetään. Tätä täsmennetään 325 §:ssä, jonka mukaan Liikenne- ja viestintävirastolla on oikeus tehdä teleyrityksessä *tekninen turvallisuustarkastus*, SVPL:n tai sen nojalla annettujen säännösten ja määräysten velvoitteiden noudattamisen valvomiseksi. Tarkastus voidaan teettä riippumattomalla asiantuntijalla. Tarkastuksen yhteydessä Liikenne- ja viestintävirastolla tai sen lukuun toimivalla tarkastajalla on oikeus päästä teleyrityksen laitetiloihin tai muihin tiloihin, sekä oikeus saada tutkittavakseen valvontatehtävän kannalta tarpeelliset asiakirjat ja tiedot.

Edellä esitellyt Liikenne- ja viestintäviraston valvontatoimivaltuudet ovat lain tasolla melko samanlaisia kuin ne, jotka Energiavirastolle on annettu sähkö- ja maakaasumarkkinoiden valvonnasta annetussa laissa. Kummallakin viranomaisella on yleinen oikeus valvoa lakien noudattamista, oikeus suorittaa tarkistus valvottavan tiloissa, sekä saada valvontaan tarvittavat tiedot. Voidaan kuitenkin perustellusti väittää, että Liikenne- ja viestintäviraston valvontatoimivaltuudet toteutuvat käytännössä paremmin kuin Energiavirastolla siitä syystä, että sillä on valtuus valvoa muiden säädösten ohella myös sen antamien, lakia täydentävien *määräysten* toteutumista. Tässä yhteydessä on mielenkiintoista jälleen huomata, että valvontatoimivaltuuksien käytännön toteutuminen ei siis riipu pelkästään siitä, mitä itse valvonnasta on säädetty laissa, vaan paljolti myös siitä, miten kattavasti valvonnan kohteena olevasta toiminnasta on säädetty.

Kyberturvallisuusvelvoitteiden noudattamatta jättämisestä seuraavista *sanktioista* säädetään muun muassa SVPL:n 330 §:ssä. Säännöksen mukaan Liikenne- ja viestintävirasto voi kyseisen lain mukaisia tehtäviä hoitaessaan antaa *huomautuksen* sille, joka rikkoo sähköisen viestinnän palveluista annettua lakia tai sen nojalla annettuja säännöksiä ja määräyksiä. Pykälän mukaan Liikenne- ja viestintävirasto voi myös *velvoittaa toimijan korjaamaan virheensä tai laiminlyöntinsä* kohtuullisessa määräajassa.

Lisäksi 331 §:ssä säädetään, että mikäli toimijan virhe tai laiminlyönti aiheuttaa välitöntä ja vakavaa vaaraa yleiselle turvallisuudelle, vakavaa taloudellista tai toiminnallista haittaa

muille yrityksille ja käyttäjille taikka viestintäverkkojen ja -palveluiden toiminnalle, Liikenne- ja viestintävirasto voi viipymättä päättää tarvittavista *väliaikaisista toimista,* 330 §:n mukaisesta määräajasta riippumatta. Liikenne- ja viestintäviraston on ennen väliaikaisia toimia koskevan päätöksen antamista varattava sen saajalle tilaisuus tulla kuulluksi, paitsi jos kuulemista ei voida toimittaa niin nopeasti kuin asian kiireellisyys välttämättä vaatii. Pykälässä tarkennetaan, että väliaikaisena toimena Liikenne- ja viestintävirasto voi keskeyttää vaaraa tai vakavaa haittaa aiheuttavan toiminnan tai määrätä muista tarpeellisista pakkokeinoista. Lain 332 §:ssä säädetään lisäksi, että Liikenne- ja viestintävirasto voi asettaa edellisten pykälien tehosteeksi *uhkasakon*, *keskeyttämisuhan* tai *teettämisuhan*.

Ankarimmasta sanktiosta säädetään SVPL:n 340 §:ssä, ja sen mukaan Liikenne- ja viestintävirasto *voi kieltää teleyritykseltä teletoiminnan harjoittamisen*, mikäli yritys edellä esiteltyjen pykälien mukaisista seuraamuksista huolimatta, rikkoo vakavasti ja olennaisesti lain säännöksiä tai sen nojalla annettuja määräyksiä.

4.2 Finanssimarkkinoiden kyberturvallisuussääntely

Heti tämän luvun alkuun on hyvä tuoda ilmi, että yhdessä NIS2 -direktiivin kanssa, EU:ssa hyväksyttiin uusi *asetus finanssialan digitaalisesta häiriönsietokyvystä*[121]. Kyseinen asetus on erityislainsäädännön asemassa suhteessa NIS2 -direktiiviin ja siinä määrätään finanssialan toimijoille erityisen tarkkoja kyberturvallisuusvelvoitteita. Asetuksen soveltaminen alkaa kuitenkin vasta 17.01.2025, joten tässä luvussa tarkastellaan vain tämänhetkistä oikeustilaa.

Finanssimarkkinoiden toimijat ovat vastuussa yhteiskunnan rahoitus- ja maksujärjestelmistä, joten monet alan yritykset voidaan katsoa kriittisiksi toimijoiksi. Finanssialan toimijoita ovat muun muassa *luottolaitokset (esimerkiksi pankit)*, *sijoituspalveluyritykset*, *rahastoyhtiöt* sekä *pörssi* ja *muut arvopapereiden kauppapaikat*.

Finanssimarkkinoiden sääntely ja valvonta on hyvin yhdenmukaistettua Euroopan unionissa.[122] EU-tasolla on annettu useita alaa ohjaavia asetuksia ja direktiivejä, sekä näitä tarkentavia komission delegoituja asetuksia. Sääntelyvaraa alan isoista linjoista on siis

[121] Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554, annettu 14 päivänä joulukuuta 2022 finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011 muuttamisesta.

[122] HE 192/2017 vp., s. 19.

kansallisella tasolla vähän, mutta Suomen lainsäädännöstä löytyy kuitenkin useita lakeja, joilla täsmennetään EU-tasoista sääntelyä. Tässä luvussa tarkastellaan nimenomaan finanssimarkkinoiden kansallista sääntelyä, keskittyen *luottolaitoksia* koskevaan kyberturvallisuuden velvoitesääntelyyn.

Kansallisen lain tasolla, luottolaitosten kyberturvallisuussääntelyssä puhutaan terminologisesti *operatiivisesta riskistä*. Käsitteellä tarkoitetaan muun muassa riskiä, joka aiheutuu riittämättömistä tai epäonnistuneista sisäisistä prosesseista, henkilöstöstä, järjestelmistä tai ulkoisista tekijöistä. Esimerkiksi luottolaitoksen verkko- ja tietojärjestelmiin kohdistuvat kyberuhat voidaan katsoa kuuluvaksi käsitteen alle.[123]

Operatiivisten riskien hallinnasta säädetään *luottolaitostoiminnasta annetun lain (610/2014)* 9 luvun 16 §:ssä, ja sen mukaan luottolaitoksella on oltava menetelmät operatiivisten riskien tunnistamiseksi, arvioimiseksi ja hallitsemiseksi. Laitoksen täytyy kuvata selkeästi, mitä se pitää operatiivisina riskeinä, ja sillä on oltava operatiivisten riskin hallintaa koskevat kirjalliset toimintaperiaatteet ja menettelytavat.

Kyseisen pykälän toisessa momentissa viitataan myös suoraan tietojärjestelmien turvallisuuteen. Säännöksen mukaan luottolaitoksella on oltava *riittävät, turvalliset ja toimintavarmat maksu-, arvopaperi- ja muut tietojärjestelmät*. Lain esitöiden mukaan tällaisina turvallisina ja toimintavarmoina järjestelminä voitaisiin pitää esimerkiksi sellaisia järjestelmiä, joissa hyödynnetään varmuuskopiointiin, varajärjestelmiin ja tietojärjestelmien suojaamiseen liittyviä alan parhaita käytänteitä.[124]

Lisäksi luottolaitostoiminnasta annetun lain 9 luvun 24 §:n mukaan *Finanssivalvonta* voi antaa *tarkempia määräyksiä* 16 §:ssä tarkoitetusta operatiivisesta riskistä. Finanssivalvonta onkin antanut tällaisen määräyksen[125], jonka 6 luvussa käsitellään luottolaitoksia koskevia tarkempia kyberturvallisuusvaatimuksia.

Määräyksessä muun muassa edellytetään, että valvottavan yrityksen *yleisen tietoturvallisuuden tason* on oltava riittävä valvottavan toiminnan luonteeseen ja laajuuteen,

---

[123] HE 192/2017 vp., s. 19.

[124] HE 39/2014 vp., s. 67.

[125] Finanssivalvonta, Määräykset ja ohjeet 8/2014, Operatiivisen riskin hallinta rahoitussektorin valvottavissa, FIVA 8/01.00/2014.

kyberuhkien vakavuuteen sekä yleiseen tekniseen kehitystasoon nähden.[126] On huomionarvoista, että samassa kohdassa määrätään myös, että nimenomaan valvottavan yrityksen *hallitus* on vastuussa tietoturvallisuuden riittävästä tasosta. Valvottavan yrityksen tulee antaa riittävät resurssit sekä määritellä vastuut tietoturvallisuuden ylläpitämiseksi. Tietoturvallisuuden tasoa tulee myös valvoa säännöllisesti ja havaittujen puutteiden korjaamiseen tulee ryhtyä välittömästi.

Vaatimus yrityksen hallituksen vastuusta on mielenkiintoinen ja potentiaalisesti hyvinkin toimiva keino kannustaa yritystä huolehtimaan kyberturvallisuudestaan. On huomionarvoista, että esimerkiksi Puolan kansallisesta kybersääntelystä löytyy jo nykyisellään tämänkaltaisia, kaikkia NIS-direktiivin soveltamisalaan kuuluvia toimijoita velvoittavia säännöksiä.[127] Asiaa on pohdittu myös EU-tasolla, ja vaatimus organisaation johdon vastuusta kyberturvallisuusvelvoitteiden noudattamisesta ollaan ottamassa laajemminkin käyttöön kriittisillä toimialoilla, NIS2 -direktiivin implementoinnin myötä. Aiheeseen palataan vielä uudestaan tutkielman luvussa 5.2.

Finanssivalvonnan määräyksessä annetaan myös muita tarkempia velvoitteita liittyen esimerkiksi tietojärjestelmien käyttöoikeuksiin, tietoturvariskien hallintaan, tietoturvallisuutta koskevaan ohjeistukseen ja koulutukseen, tietoturvallisuuden varmistamiseen tietoverkoissa sekä tietoturvallisten palveluiden kehittämiseen.

Kuten huomataan, myös finanssimarkkinoiden osalta kyberturvallisuusvelvoitteiden varsinainen vaikuttavuus saavutetaan vasta lainsäädäntöä tarkentavien määräysten myötä. Samoin kuin sähköverkkojen kohdalla, myöskään finanssimarkkinoiden kyberturvallisuussääntely ei ole lain tasolla mitenkään erityisen yksityiskohtaista, mutta juuri Finanssivalvonnalle annettu määräyksenantovaltuus tekee siitä käytännön tasolla velvoittavampaa.

4.3 Terveydenhuoltoalan kyberturvallisuussääntely

Finanssimarkkinoiden ohella toinen huomionarvoinen ja yhteiskunnan toiminnan kannalta kriittinen toimiala on *terveydenhuoltoala*. Tässä luvussa keskitytään kuvaamaan

[126] Finanssivalvonta 2014, s. 23.

[127] Chałubińska-Jentkiewicz – Radoniewicz – Zieliński 2022, s. 378–380.

kyberturvallisuussääntelyä, joka kohdistuu terveydenhuoltoalalla käytettäviin asiakastietojärjestelmiin. Aiheeseen liittyvä merkittävin säädös on *sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annettu laki (784/2021)*.

Laki on melko uusi, ja siinä säädetään kattavasti asiakastietojen sähköiseen käsittelyyn tarkoitettujen tietojärjestelmien sekä hyvinvointisovellusten *olennaisista vaatimuksista*, sekä sosiaali- ja terveydenhuollon palvelujenantajien *tietoturvallisuuden omavalvonnasta*.

Säännöksissä asetetaan velvoitteita *sosiaali- ja terveydenhuollon palvelunantajille*, joilla tarkoitetaan käytännössä monia julkisia ja yksityisiä sosiaali- ja terveyspalveluja tarjoavia organisaatiota. Lisäksi laissa asetetaan velvoitteita *tietojärjestelmäpalveluiden tuottajille* ja *hyvinvointisovellusten valmistajille*, jotka ovat käytännössä niitä yrityksiä, jotka vastaavat itse tietojärjestelmien ja sovellusten kehittämisestä.

Lain 34 §:n mukaan asiakastietojen käsittelyssä käytettävän tietojärjestelmän ja hyvinvointisovelluksen tulee täyttää *yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä toiminnallisuutta koskevat olennaiset vaatimukset*. Pykälän mukaan tietojärjestelmä täyttää olennaiset vaatimukset silloin, kun se on suunniteltu, valmistettu ja toimii tietoturvaa ja tietosuojaa koskevien lakien ja niiden nojalla annettujen säännösten sekä yhteentoimivuutta koskevien kansallisten määrittelyjen mukaisesti. *Terveyden ja hyvinvoinnin laitos* voi lisäksi antaa tarkempia määräyksiä näiden olennaisten vaatimusten sisällöstä.

Lain esitöiden mukaan tietoturvaa ja tietosuojaa koskevat vaatimukset takaisivat sen, että tiedot tallentuisivat ja säilyisivät muuttumattomina, ja salassa pidettäviä tietoja pääsisivät käsittelemään vain henkilöt, joilla on siihen lakiin perustuva oikeus.[128] Muuten esitöissä ei merkittävästi täsmennetä tätä melko yleisluonteista 34 §:ää, mutta olennaiset vaatimukset konkretisoituvat tässäkin tapauksessa THL:n antaman *määräyksen*[129] myötä. Määräys lukuisine liitteineen on hyvin kattava, ja yhdessä muiden THL:n antamien määräysten kanssa määrittelee erittäin yksityiskohtaisesti tietojärjestelmien ja hyvinvointisovellusten tietoturvallisuutta ja tietosuojaa koskevat vaatimukset.

---

[128] HE 212/2020 vp., s. 118.

[129] Terveyden ja hyvinvoinnin laitos, Määräys 5/2021: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista, THL/4311/4.09.00/2021, 9.12.2021.

Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain 35 §:n mukaan luokkaan A kuuluvan tietojärjestelmän ja hyvinvointisovelluksen vaatimustenmukaisuus on myös osoitettava *sertifioinnilla*, jonka hankkimisesta vastaa tietojärjestelmäpalvelun tuottaja tai hyvinvointisovelluksen valmistaja. Tässä yhteydessä sertifioinnilla tarkoitetaan eräänlaista *todistusta* siitä, että järjestelmä täyttää muun muassa sille asetetut tietoturvavaatimukset.

Terveyden ja hyvinvoinnin laitos voi myös antaa tarkempia määräyksiä sertifiointimenettelystä ja sertifiointien sisällöstä, ja THL onkin jälleen käyttänyt määräyksenantovaltuuttaan[130]. Lain 37 §:ssä lisäksi tarkennetaan sertifiointivelvoitetta niin, että vaadittava sertifikaatti myönnetään erillisen *tietoturvallisuuden arviointilaitoksen* suorittaman arvioinnin perusteella.

Kyseinen vaatimus erillisen sertifikaatin hankkimisesta terveydenhuollon merkittävälle asiakastietotietojärjestelmälle on vielä tällä hetkellä harvinainen poikkeus kriittisten toimialojen kyberturvallisuussääntelyssä. Liikenne- ja viestintäministeriö onkin raportissaan Tietoturvan ja tietosuojan parantamisesta yhteiskunnan kriittisillä toimialoilla todennut, että sertifiointivaatimukset voisivat olla hyvä keino lisätä kyberturvallisuutta kaikilla kriittisillä toimialoilla[131]. Raportissa viitataan esimerkinomaisesti *ISO 27001 -sertifikaattiin*, joka keskittyy erityisesti siihen, miten tietoturva on hallinnollisesti järjestetty organisaatiossa ja sen toiminnassa.

Ministeriö nostaa myös esille *tietosuojaan* liittyvät sertifioinnit, ja raportin mukaan ulkopuolisten riippumattomien sertifiointielinten tekemät arviot lisäisivät toiminnan uskottavuutta, laajentaisivat merkittävästi mahdollisuuksia tietosuojavelvoitteiden noudattamisen tehokkaaseen valvontaa ja toisivat rekisterinpitäjille tärkeää osaamista tietosuojan kehittämiseen[132]. Tietoturvaan liittyvillä sertifioinneilla olisi eittämättä samanlaisia positiivisia vaikutuksia toimijan tietoturvaan, ja vaatimus tietojärjestelmien sertifioinnista voisi edistää huomattavasti myös esimerkiksi sähköverkonhaltijoiden

---

[130] Terveyden ja hyvinvoinnin laitos, Määräys 4/2021: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista, THL/4310/4.09.00/2021, 9.12.2021.

[131] Liikenne- ja viestintäministeriö 2021, s. 41.

[132] Liikenne- ja viestintäministeriö 2021, s. 43.

kyberturvallisuuden tasoa. Sertifiointivaatimuksiin yhtenä keinona parantaa organisaation kyberturvallisuutta palataan vielä luvussa 5.3.3.

Itse asiakastietojärjestelmien sekä hyvinvointisovellusten tietoturva- ja sertifiointivaatimusten lisäksi, laissa säädetään myös palvelunantajien velvollisuudesta suorittaa tietoturvallisuuden ja tietosuojan *omavalvontaa.* Lain 27 §:n mukaan terveydenhuoltoalan toimijan on laadittava tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä *tietoturvasuunnitelma*. Suunnitelmassa on oltava selvitykset muun muassa siitä, että 1) tietojärjestelmien käyttäjillä on käyttöön vaadittu koulutus, 2) tietojärjestelmien käyttöohjeet ovat asianmukaisesti saatavilla, 3) tietojärjestelmiä käytetään, ylläpidetään ja päivitetään ohjeiden mukaisesti, 4) tietojärjestelmiä asentaa, ylläpitää ja päivittää vain henkilö, jolla on siihen tarvittava ammattitaito ja asiantuntemus ja 5) tietojärjestelmät täyttävät muun muassa tietoturvaan liittyvät olennaiset vaatimukset. Pykälässä todetaan myös jälleen, että THL voi antaa tarkempia määräyksiä tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista sekä tietoturvallisuuden todentamisesta. Pykälä on mielenkiintoinen ja avaa jo lain tasolla verrattain yksityiskohtaisesti vaadittavan tietoturvasuunnitelman sisältöä. Terveyden ja hyvinvoinnin laitos on antanut myös tästä säännöksestä *tarkentavan määräyksen*[133], jossa tietoturvasuunnitelman sisältöä konkretisoidaan entisestään.

Tietoturvallisuuden omavalvonnan toteuttamista korostetaan lisäksi 28 §:ssä, jonka mukaan sosiaali- ja terveydenhuollon palvelunantajan *vastaavan johtajan* on huolehdittava, että 27 §:ssä tarkoitettu tietoturvasuunnitelma laaditaan ja sitä noudatetaan. Lain esitöissä korostetaan, että kyseisen säännöksen puitteissa jokaisen sosiaali- ja terveydenhuollon palvelunantajan olisi aktiivisesti seurattava tietoturvasuunnitelman toteutumista, jotta tietoturvaan ja tietosuojaan liittyvät asiat tulisivat hoidetuksi asianmukaisesti. Jokaisen palvelunantajan ammatillisesta toiminnasta vastaavan johtajan olisi myös annettava kirjalliset ohjeet asiakastietojen käsittelystä ja noudatettavista menettelytavoista sekä huolehdittava henkilökunnan riittävästä asiantuntemuksesta ja osaamisesta asiakastietojen käsittelyssä.[134]

Kyseinen pykälä on toinen esimerkki säännöksestä, jolla riittävästä kyberturvallisuuden tasosta huolehtiminen on vastuutettu nimenomaan tietylle yksityishenkilölle. Tämänkaltaisen

---

[133] Terveyden ja hyvinvoinnin laitos, Määräys 3/2021: Tietoturvasuunnitelmaan sisällytettävät selvitykset ja vaatimukset, THL/4309/4.09.00/2021, 20.12.2021.

[134] HE 212/2020 vp., s. 114.

säännöksen tuominen esimerkiksi sähköverkonhaltijoiden varautumissuunnittelua koskevan sähkömarkkinalain 28 §:n yhteyteen voisi omalta osaltaan edistää sähköverkonhaltijoiden kyberturvallisuusvelvoitteiden noudattamista.

5 Sähköverkkojen kyberturvallisuussääntelyn parantaminen

5.1 Kyberturvallisuussääntelyn kehittämisestä yleisesti

Seuraavissa luvuissa on tarkoitus pohtia, kuinka sähköverkkojen kyberturvallisuussääntelyä tulisi kehittää, jotta verkonhaltijat olisivat jatkossa paremmin varautuneita kyberuhkiin. Parannusehdotukset pohjautuvat edellisten lukujen lainopilliseen analyysiin sähköverkkojen kyberturvallisuussääntelyn nykytilasta, vertailusta muiden kriittisten toimialojen vastaavaan sääntelyyn, sekä kirjallisuudessa ja viranomaisjulkaisuissa esitettyihin argumentteihin.

Yleisesti ottaen tutkimukset ovat osoittaneet, että sääntelyllä on positiivinen vaikutus organisaatioiden kyberturvallisuuteen.[135] Erityisesti aloilla, joilla kattavalla kyberturvallisuussääntelyllä on pitkät perinteet, kyberturvallisuus toteutuu myös käytännön tasolla parhaiten. Esimerkkejä tällaisista aloista ovat finanssiala sekä teleliikenneala.[136]

Tarkoituksenmukaisen sääntelyn luomiseen liittyy kuitenkin paljon haasteita. Ensinnäkin kyberturvallisuussääntelyssä on omaksuttu niin sanottu *teknologianeutraliteetin periaate*. Tällä tarkoitetaan sitä, että sääntelystä ei saisi tehdä liian yksityiskohtaista, niin että se edellyttäisi esimerkiksi tiettyjen laitteiden tai kaupallisten tietoturvatuotteiden käyttöä.[137] Periaatteeseen viitataan myös esimerkiksi NIS-direktiivin johdanto-osan 51 kappaleessa.

Periaatteen taustalla on ajatus siitä, että tarkasti tiettyyn teknologiaan sidotut velvoitteet eivät toimisi jatkuvasti muuttuvassa kyberympäristössä.[138] Samalla kun tietojärjestelmien arkkitehtuuri ja kyberhyökkäyksissä käytettävä teknologia kehittyy, myös suojautumiseen käytettävän teknologian on pysyttävä perässä. Lainsäädäntö on tällaisessa tilanteessa auttamatta liian hidas väline velvoitteiden päivittämiseen, mistä syystä laintasoisessa kyberturvallisuussääntelyssä on parasta pysyä myös tulevaisuudessa yleisemmällä tasolla ja keskittyä toimenpiteiden minimivaatimuksiin.[139]

---

[135] Huoltovarmuusorganisaation Digipooli 2020, s. 19–20.

[136] Huoltovarmuusorganisaation Digipooli 2020, s. 8.

[137] Maxwell – Bourreau 2014, s. 1.

[138] Maxwell – Bourreau 2014, s. 4.

[139] Huoltovarmuusorganisaation Digipooli 2020, s. 20.

Yksityiskohtaisen laintasoisen kyberturvallisuussääntelyn haasteena on lisäksi se, että sääntelyllä pitäisi kyetä asettamaan velvoitteita hyvin erilaisille ja erikokoisille toimijoille.[140] Jopa samojen toimialojen sisällä on paljon hajontaa eri organisaatioiden välillä, ja esimerkiksi riittäviin teknisiin investointeihin tarvittavat resurssit voivat vaihdella huomattavasti yrityksestä toiseen.[141] Myöskään tietyt organisatoriset toimenpiteet eivät välttämättä sopisi kaikille toimijoille, sillä esimerkiksi organisaation rakenne ja henkilöstön määrä voivat vaihdella toimijoiden välillä. Liian tiukka sääntely voisi kankeuttaa Suomessa yleisten pienten ja keskisuurten yritysten toimintaa.[142]

Alan tutkimuksissa yhdeksi kyberturvallisuussääntelyn kehittämisen haasteeksi on tunnistettu myös niin sanottu *”asiantuntemuksen epäsuhtaisuus” (expertise asymmetry)*. Tällä tarkoitetaan sitä, että monesti paras asiantuntemus kullekin alalle soveltuvasta teknisestä sääntelystä on kriittisten toimijoiden teknisellä henkilöstöllä itsellään, eikä suinkaan lainsäätäjällä.[143] Haasteeseen vastaamiseksi on esitetty mahdollisimman syvällistä ja pitkäjänteistä yhteistyötä teknisten asiantuntijoiden, tietoturva-asiantuntijoiden sekä oikeudellisten asiantuntijoiden kesken, kyberturvallisuussääntelyn kaikissa kehitysvaiheissa.[144] Alan tutkimuksessa on myös esitetty mallia, jossa lainsäätäjä ja kriittiset toimijat laatisivat kutakin alaa koskevat kyberturvallisuussäännökset eräänlaisena *yhteissääntelynä*.[145]

Kaikista edellä mainituista lainsäädännöllisistä haasteista huolimatta, sähköverkkojen laintasoista kyberturvallisuussääntelyä voitaisiin kuitenkin kehittää. Kuten luvun 3 analyysistä käy ilmi, sähköverkonhaltijoita koskeva kyberturvallisuussääntely on tällä hetkellä hyvin yleisluonteista, epätäsmällistä ja heikosti velvoittavaa. Luvussa 4 esitetyn vertailevan analyysin pohjalta voidaan lisäksi todeta, että muilla kriittisillä toimialoilla

---

[140] Wong 2018, s. 269.

[141] Helsingin seudun kauppakamari 2019, s. 21–22; Huoltovarmuusorganisaation Digipooli 2020, s. 21

[142] Huoltovarmuusorganisaation Digipooli 2020, s. 20.

[143] Michalec – Milyaeva – Rashid 2022, s. 1329.

[144] Michalec – Milyaeva – Rashid 2022, s. 1326

[145] Sales 2013, s. 1554–1557.

kyberturvallisuussääntely on selvästi tarkempaa ja velvoittavampaa, ja näistä aloista voitaisiinkin ottaa mallia sähköverkkojen sääntelyn parantamiseen.

Sääntelyn kehittämisen puolesta puhuu myös sähköverkkojen yleisesti tunnustettu kriittinen asema yhteiskunnassa. Verkkojen toiminta ja turvallisuus on elintärkeää niin muiden kriittisten toimijoiden, kuin myös kaikkien muiden tahojen kannalta. Aiempaa ankarammat kyberturvallisuusvelvoitteet lisäisivät toki sähköverkonhaltijoiden hallinnollista taakkaa sekä kyberturvallisuusinvestointeihin tarvittavia kustannuksia niin lyhyellä kuin pitkälläkin aikavälillä. Esimerkiksi investoinnit uusiin laitteisiin, tietoturvayhtiöiden palveluihin sekä työntekijöiden jatkuvaan koulutukseen tulisivat eittämättä kalliiksi. Tästäkin huolimatta, lainsäätäjän pitäisi kyetä perustelemaan sääntelyyn tehtävät tiukennukset, sillä yhteiskunnan kokonaisturvallisuuden voidaan ajatella painavan tässä kohtaa vaakakupissa enemmän.

Myös liikenne- ja viestintäministeriö on raportissaan Tietoturvan ja tietosuojan parantamisesta yhteiskunnan kriittisillä toimialoilla korostanut sääntelyn kehittämistä ensisijaisena keinona lisätä kriittisten toimijoiden kyberturvallisuutta.[146] On myös huomionarvoista, että raportissa sekä sen perusteella annetussa valtioneuvoston periaatepäätöksessä, nimenomaan sähköverkonhaltijoita korostetaan suhteessa muihin kriittisiin toimijoihin.[147] Myös Energiavirasto kannattaa sähköverkkojen kyberturvallisuussääntelyn kehittämistä entistä täsmällisemmäksi.[148]

5.2 Euroopan unionin uusi kyberturvallisuusdirektiivi (NIS2 -direktiivi)

Aiemmissa luvuissa on viitattu useasti EU:n uuteen *kyberturvallisuusdirektiiviin (NIS2 -direktiivi)*, jolla tullaan korvaamaan nykyisin voimassa oleva verkko- ja tietoturvadirektiivi (NIS-direktiivi). Uuden direktiivin myötä voimme odottaa huomattavia parannuksia kriittisten toimialojen kyberturvallisuussääntelyyn. Jo näillä parannuksilla voidaan mitä todennäköisimmin vastata moniin niistä sähköverkkojen kyberturvallisuussääntelyn puutteista, joita tässä tutkimuksessa on nostettu esille. Seuraavaksi käydään läpi sähköverkonhaltijoita koskevien velvoitteiden kannalta merkittävimpiä direktiivin uudistuksia. NIS2 -direktiivi sisältää tässä esitettävien asioiden lisäksi myös monia muita

[146] Liikenne- ja viestintäministeriö 2021, s. 50–51.

[147] Valtioneuvosto 2021, s. 8.

[148] Energiavirasto 2021, s. 1.

uudistuksia, liittyen esimerkiksi direktiivin soveltamisalaan, kriittisten toimijoiden määrittelemiseen sekä viranomaisyhteistyöhön.

Uuden direktiivin 20 artiklassa annetaan säännös, jonka mukaan kriittisen toimijan *hallintoelin* on velvoitettava vastaamaan siitä, että organisaatiossa todella noudatetaan direktiivin mukaisia kyberturvallisuusriskien hallintatoimenpiteitä. Hallintoelimen tulisi valvoa velvoitteiden noudattamista, ja se voitaisiin asettaa vastuuseen, mikäli organisaatio olisi laiminlyönyt velvoitteensa. Saman artiklan mukaan hallintoelimen tulisi myös pitää yllä kyberturvallisuuteen liittyvää tietotaitoaan osallistumalla asianmukaisiin koulutuksiin.

Uudistus on mielenkiintoinen ja se voisi huomattavastikin lisätä organisaatioiden kyberturvallisuutta. Yksittäisten johtohenkilöiden asettaminen henkilökohtaiseen vastuuseen laiminlyönneistä voisi toimia tehokkaana kannusteena riittävien kyberturvallisuustoimien omaksumiselle. Uudistus tulisi todennäköisesti edellyttämään laintasoisia muutoksia kaikille direktiivin alaisille toimialoille, ja kansallisessa lainsäädännössä pitäisi myös todennäköisesti säätää tarkemmin niistä henkilöistä, joita vastuu tulisi koskemaan. Vastuu voisi kohdistua esimerkiksi yrityksen toimitusjohtajaan tai hallituksen jäseniin.

Uudessa direktiivissä täsmennetään ja laajennetaan huomattavasti *kyberturvallisuusriskien hallintaan* liittyviä velvoitteita. Direktiivin 21 artiklan mukaan toimijoiden on toteutettava asianmukaiset ja oikeasuhteiset tekniset, operatiiviset ja organisatoriset toimenpiteet hallitakseen niihin kohdistuvia kyberturvallisuusriskejä. Toimenpiteitä toteutettaessa olisi otettava huomioon viimeisin kehitys, tapauksen mukaan asiaa koskevat eurooppalaiset ja kansainväliset standardit sekä täytäntöönpanokustannukset. Toimenpiteet on myös suhteutettava toimijan tietojärjestelmiin kohdistuviin riskeihin.

Vaadittavia toimenpiteitä täsmennetään siten, että niiden tulisi sisältää vähintään: a) riskianalyysit ja tietojärjestelmien turvallisuutta koskevat politiikat, b) poikkeamien käsittelyn, c) toiminnan jatkuvuuden hallinnan, kuten esimerkiksi varmuuskopioiden käytön ja palautumissuunnittelun sekä kriisinhallinnan, d) toimitusketjujen turvallisuuden, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat, e) verkko- ja tietojärjestelmien hankkimiseen, kehittämiseen ja ylläpitämiseen liittyvät turvallisuusseikat, mukaan lukien haavoittuvuuksien käsittelyn ja julkistamisen, f) toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta, g) perustason kyberhygieniakäytännöt ja

kyberturvallisuuskoulutuksen, h) toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä, i) henkilöstöturvallisuuden, pääsynhallintaperiaatteet ja omaisuudenhallinnan, sekä j) tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käytön toimijan toiminnassa.

Perustason kyberhygieniakäytäntöjä täsmennetään direktiivin johdanto-osan 49 kappaleessa, ja niihin katsotaan kuuluvaksi muun muassa yhteiset perustason käytännöt, kuten ohjelmisto- ja laitteistopäivitykset, salasanojen vaihtaminen, uusien asennusten hallinta, ylläpitäjän käyttöoikeuksia edellyttävien tilien rajoittaminen sekä tietojen varmuuskopiointi. Komissiolle on myös valta antaa *tarkempia täytäntöönpanosäädöksiä* edellä mainituista toimenpiteistä.

Kuten voidaan huomata, uudessa direktiivissä säädetään hyvin kattavasti vaadittavista riskienhallintatoimenpiteistä. Aikaisemmin tämän tasoista sääntelyä on löytynyt Suomessa lähinnä toimivaltaisten viranomaisten antamista *määräyksistä*, ja nyt tarkat velvoitteet on siirretty kerta heitolla EU-sääntelyn tasolle. Näin ollen uusien säännösten implementoiminen tulee todennäköisesti vaatimaan merkittäviä täsmennyksiä kansalliseen lainsäädäntöön kaikilla kriittisillä toimialoilla, myös sähkömarkkinalain säännöksiin sähköverkonhaltijoiden osalta.

Kyberturvallisuusriskien hallintaan liittyvien toimenpiteiden lisäksi myös *poikkeamista raportoimiseen* liittyviä velvoitteita on täsmennetty NIS2 -direktiivissä. Raportointi on esimerkiksi 23 artiklassa muutettu monivaiheiseksi prosessiksi, jossa organisaation on ensimmäiseksi annettava *ennakkovaroitus* tapahtuneesta poikkeamasta, tämän jälkeen varsinainen *ilmoitus* ja tarvittaessa *väliraportti*, sekä viimeistää kuukauden kuluessa ilmoituksesta kattavampi *loppuraportti* tapahtuneesta poikkeamasta. Uudistuksen myötä ilmoitukset on tehtävä ensisijaisesti SCIRT-toimijalle (Kyberturvallisuuskeskukselle) ja vain tarvittaessa toimivaltaiselle viranomaiselle (Energiavirasto).

Uudessa direktiivissä on myös merkittävästi täsmennetty viranomaisten *valvontatoimivaltuuksia* sekä velvoitteiden rikkomisesta seuraavia *sanktioita*. Direktiivin 32 artiklan mukaan toimivaltaisilla viranomaisilla tulee olla *valvontatehtäviään* hoitaessa valtuudet ainakin seuraaviin: a) koulutettujen ammattilaisten toteuttamat paikalla tehtävät tarkastukset ja muu kuin paikalla toteutettava valvonta, mukaan lukien satunnaistarkastukset, b) riippumattoman elimen tai toimivaltaisen viranomaisen suorittamat säännölliset ja

kohdennetut turvallisuusauditoinnit, c) tapauskohtaiset auditoinnit, myös kun perusteena on merkittävä poikkeama tai se, että keskeinen toimija on rikkonut direktiiviä, d) objektiivisiin, syrjimättömiin, oikeudenmukaisiin ja läpinäkyviin riskinarviointikriteereihin perustuvat turvallisuusskannaukset, tarvittaessa yhteistyössä asianomaisen toimijan kanssa, e) pyynnöt saada tietoja, jotka ovat tarpeen asianomaisen toimijan hyväksymien kyberturvallisuusriskien hallintatoimenpiteiden arvioimiseksi, mukaan lukien dokumentoidut kyberturvallisuusperiaatteet, f) pyynnöt saada pääsy dataan, asiakirjoihin ja tietoihin, joita tarvitaan valvontatehtävien suorittamiseksi, sekä g) pyynnöt saada näyttöä kyberturvallisuusperiaatteiden täytäntöönpanosta, kuten pätevän tarkastajan suorittamien turvallisuusauditointien tulokset ja niiden perustana oleva näyttö.

Lisäksi 32 artiklassa edellytetään, että toimivaltaisilla viranomaisilla tulee olla *täytäntöönpanovaltuudet* ainakin seuraaviin: a) antaa varoituksia, kun toimijat rikkovat direktiiviä, b) antaa toimijoille sitovia ohjeita poikkeamien ehkäisemiseksi tai korjaamiseksi, c) määrätä asianomaiset toimijat lopettamaan tämän direktiivin vastainen toiminta ja pidättäytymään tästä toiminnasta vastaisuudessa, d) määrätä asianomaiset toimijat varmistamaan, että niiden kyberturvallisuusriskien hallintatoimenpiteet ovat 21 artiklan mukaisia, tai täyttämään 23 artiklassa säädetyt raportointivelvoitteensa määrätyllä tavalla ja määrätyn ajan kuluessa, e) määrätä asianomaiset toimijat tiedottamaan niille luonnollisille henkilöille tai oikeushenkilöille, joille ne tarjoavat palvelujaan tai toimintojaan ja joihin merkittävä kyberuhka saattaa vaikuttaa, uhkan luonteesta sekä mahdollisista suojatoimenpiteistä tai korjaavista toimenpiteistä, f) määrätä asianomaiset toimijat panemaan täytäntöön turvallisuusauditoinnin tuloksena annetut suositukset kohtuullisessa määräajassa, g) nimetä valvova virkamies, joka valvoo tarkoin määriteltyjen tehtävien puitteissa määräkauden ajan, että asianomaiset toimijat noudattavat 21 ja 23 artiklaa, h) määrätä asianomaiset toimijat julkistamaan määrätyllä tavalla seikat, jotka liittyvät tämän direktiivin rikkomiseen, sekä i) määrätä tai pyytää asiaankuuluvia elimiä tai tuomioistuimia määräämään kansallisen lainsäädännön mukaisesti hallinnollisia sakkoja 34 artiklan nojalla minkä tahansa tämän kohdan a–h alakohdassa tarkoitetun toimenpiteen lisäksi.

Kyseisessä 34 artiklassa säädetään hyvin kattavasti *hallinnollisista sakoista*, joita toimivaltaisten viranomaisten on määrättävä toimijoille, jotka ovat rikkoneet direktiivin mukaisia velvoitteitaan. Artiklassa määritellään rahamääräiset rajat sakoille. Kuten luvussa 3.3.3 todettiin, tämänkaltaisia säännöksiä on ollut jo aiemmin monissa muissa EU-maissa, mutta ei Suomessa.

5.3 Muutosehdotuksia kansalliseen sääntelyyn

5.3.1 Muutosehdotuksia sähkömarkkinalakiin ja valvontalakiin

Luvussa 3 tarkasteltiin sähköverkkojen kansallista kyberturvallisuussääntelyä, jonka tärkeimpinä säädöksinä ovat *sähkömarkkinalaki* sekä *laki sähkö- ja maakaasumarkkinoiden valvonnasta (valvontalaki)*. Lainopillisen analyysin perusteella päädyttiin siihen lopputulokseen, että kyseinen sääntely on tällä hetkellä riskienhallintavelvoitteiden osalta heikosti velvoittavaa ja vaillinaista. Tässä luvussa esitetään muutamia konkreettisia kehitysehdotuksia sähkömarkkinalain ja valvontalain relevantteihin pykäliin. Ehdotukset ovat vain esimerkkejä, ja lainsäätäjä saattaa päätyä tekemään toisenlaisia muutoksia kansalliseen lainsäädäntöömme, esimerkiksi NIS2 -direktiivin implementoinnin yhteydessä.

Sähkömarkkinalain 19 §:ssä säädetään verkonhaltijan velvollisuudesta kehittää hallitsemaansa verkkoa sekä varmistaa sen turvallisuus ja sähköntoimituksen laatu. Kuten luvussa 3.2.4 argumentoitiin, pykälä ei tällä hetkellä tunnu velvoittavan kyberturvallisuuden huomioimiseen sähköverkkojen suunnittelun, rakentamisen ja ylläpidon yhteydessä. Säännöstä voidaan verrata sähköisen viestinnän palveluista annetun lain 243 §:ään, jossa säädetään samankaltaisista velvoitteista viestintäverkkojen ja -palveluiden osalta. Kyseisessä pykälässä käsitellään kyberturvallisuudesta huolehtimista monistakin eri näkökulmista. Sähkömarkkinalain 19 §:ään voitaisiin perustellusti lisätä samankaltaiset velvoitteet kyberturvallisuudesta huolehtimiseksi, toki huomioiden alan omat erityispiirteet.

Sähkömarkkinalain 29 a §:ssä säädetään sähköverkonhaltijoiden velvollisuudesta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. Kuten luvussa 3.2.5 argumentoitiin, säännös on jopa sen taustalla olevaan NIS-direktiivin 14 artiklaan verrattuna muotoilultaan hyvin yleisellä tasolla, eikä sellaisenaan velvoita konkreettisiin toimenpiteisiin. Pykälä kaipaisikin merkittävää täsmennystä. Kuten edellä NIS2 -direktiivin mukaisia uudistuksia käsiteltäessä todettiin, kyberturvallisuusriskienhallinnan sääntely on joka tapauksessa lähitulevaisuudessa muuttumassa, joten voimme näiltä osin odottaa myös sähkömarkkinalain 29 a §:ään merkittäviä täsmennyksiä direktiivin implementoinnin yhteydessä.

Kyseiseen pykälään voisi olla perusteltua myös lisätä esimerkiksi velvoite *dokumentoida* organisaatiossa omaksutut riskienhallintatoimenpiteet ja liittää ne osaksi 28 §:n mukaista varautumissuunnitelmaa. Tällä hetkellä 29 a §:ssä ei mainita mitään vaadittavien

riskinhallintatoimenpiteiden dokumentoimisesta; tosin lain esitöiden pykäläkohtaisissa perusteluissa todetaan, että riskienhallinnan tulisi olla todennettavassa muodossa.[149] Toimenpiteiden dokumentointivelvoitteen lisääminen itse pykälätekstiin voisi kuitenkin olla perusteltua, sillä se korostaisi kyberturvallisuustoimenpiteiden merkitystä ja pakottaisi toimijat suunnittelemaan riskinhallintatoimenpiteitä entistä perusteellisemmin. Lisäksi, kuten lain esitöissäkin todetaan, dokumentointi helpottaisi valvontaviranomaisten toimintaa.[150] Organisaatioiden kyberturvallisuuden hallintaa käsittelevässä kirjallisuudessa on myös korostettu kattavan dokumentoinnin merkitystä sille, että vaadittuihin kyberturvallisuustoimiin myös ryhdytään käytännön tasolla.[151]

Dokumentoinnista puheen ollen, sähkömarkkinalakiin voisi olla perusteltua lisätä myös pykälä organisaation velvollisuudesta laatia erillinen *kyberturvallisuusstrategia*. Tämä eroaisi kirjallisesta varautumissuunnittelusta siinä mielessä, että se keskittyisi yksityiskohtaisten toimenpiteiden kuvausten sijaan kyberturvallisuuden pitkän aikavälin suunnitteluun ja kehittämiseen. Pitkän tähtäimen suunnitelmien, joissa asetetaan kyberturvallisuuden tavoitteet ja vastuut, on todettu kannustavan erityisesti organisaation johtoa sitoutumaan kyberturvallisuustoimenpiteisiin.[152] Juurikin johdon sitoutumisella on myös katsottu olevan merkittäviä positiivisia vaikutuksia organisaation kyberturvallisuuteen pitkällä aikavälillä.[153] Velvollisuus erillisen strategian laatimiseen olisi toki jälleen yksi uusi hallinnollinen rasite, joten sen tarkoituksenmukaisuutta pitäisi harkita hyvin tarkasti.

Luvussa 3.3.3 todettiin, että valvontalain kyberturvallisuusvelvoitteisiin liittyvät sanktiosäännökset ovat nykyisellään puutteellisia. Esimerkiksi lain *seuraamusmaksua* käsittelevässä 16 §:ssä ei viitata lainkaan sähkömarkkinalain kyberturvallisuussäännöksiin. Näin ollen Energiavirastolla ei ole tällä hetkellä valtuutta määrätä seuraamusmaksua näiden velvoitteiden laiminlyömisestä. Tilanne voitaisiin korjata yksinkertaisesti siten, että pykälään lisättäisiin viittaukset sähkömarkkinalain 28 ja 29 a §:iin. NIS2 -direktiivin implementoiminen tulee mitä todennäköisimmin johtamaan tässä kappaleessa esiteltyihin

---

[149] HE 192/2017 vp., s. 77.

[150] HE 192/2017 vp., s. 77–78.

[151] Bayuk ym. 2012, s. 77–79.

[152] Huoltovarmuusorganisaation Digipooli 2020, s. 7.

[153] Bayuk ym. 2012, s. 69–70.

muutoksiin, sillä direktiivin 33 ja 34 artiklassa edellytetään jäsenvaltiot varmistamaan, että toimivaltaisilla viranomaisilla on oikeudet määrätä toimijoille vaikuttavia, oikeasuhteisia ja varoittavia *hallinnollisia sakkoja*. Lisäksi itse Energiaviraston valvontatoimivaltuutta juuri kyberturvallisuusvelvoitteisiin liittyen voitaisiin selkeyttää valvontalaissa. Energiaviraston tosiasialliset mahdollisuudet tehokkaaseen valvontaan lisääntyisivät myös varmasti jo sen myötä, että itse velvoitesäännöksiä saataisiin täsmennettyä edellä esitetyllä tavalla.

5.3.2 Energiaviraston määräyksenantovaltuus

Ehkä merkittävin yksittäinen parannus sähköverkkojen kyberturvallisuussääntelyyn olisi se, että Energiavirastolle annettaisiin sähkömarkkinalaissa valtuus antaa tarkentavia *määräyksiä* vaadittavista kyberturvallisuustoimista. Nykyisellään Energiavirasto on joutunut tyytymään suositusluonteisiin *ohjeisiin*. Kuten luvussa 3.2.6 tuotiin esille, valtuudesta antaa sitovia määräyksiä on aina säädettävä lain tasolla. Lisäys voitaisiin tehdä esimerkiksi sähkömarkkinalain 28 sekä 29 a §:iin.

Edellä luvussa 5.1 argumentointiin, että tarkkojen laintasoisten kyberturvallisuussäännösten laatiminen on hankalaa, muun muassa teknologianeutraliteetin periaatteesta sekä sääntelyn kohteena olevien organisaatioiden moninaisuudesta johtuen. Toimivaltaisen viranomaisen antama määräys vaikuttaakin olevan tällä hetkellä toimivin säädöstyyppi tarkempien kyberturvallisvelvoitteiden asettamiseen. Määräyksissä kyberturvallisuusvelvoitteita voitaisiin kohdistaa lakia tarkemmin vain tiettyihin toimijoihin, ja esimerkiksi tarkoituksenmukaisista teknisistä ja organisatorisista toimenpiteistä voitaisiin säätää joustavammin lain sijasta viranomaisen antamassa määräyksessä. Kyberturvallisuussääntelyn kannalta paras tilanne voitaisiinkin saavuttaa siten, että velvoitteista säädettäisiin ensin laintasolla melko kattavasti, ja tämän lisäksi olisi laissa vielä säädetty toimivaltaiselle viranomaiselle valtuus antaa tarkentavia määräyksiä vaadittavista toimenpiteistä.[154]

Määräysten toimivuuden puolesta puhuu myös se, että niitä on helpompaa ja nopeampaa muuttaa kuin eduskuntatasoisia lakeja. Tämä puolestaan sopii hyvin kyberympäristöön, joka itsekin on aiemmin todetulla tavalla jatkuvassa muutoksessa. Lisäksi esimerkiksi Energiavirastolla olisi mitä todennäköisimmin (ainakin yhteistyössä Kyberturvallisuuskeskuksen kanssa) paras asiantuntemus merkittävistä kyberturvallisuuteen

[154] Liikenne- ja viestintäministeriö 2021, s. 50–51.

liittyvistä seikoista sekä realiteeteista juuri sähköverkkojen toimialalla, mistä syystä se olisi myös paras taho luomaan tarkempaa sääntelyä alalle.[155] Kuten luvussa 4 tuotiin esille, toimivaltaisen viranomaisen antamat määräykset on todettu toimiviksi ratkaisuiksi myös muilla kriittisillä toimialoilla, kuten finanssimarkkinoilla ja televiestintäalalla. Näin ollen olisi perusteltua, että sama käytäntö tuotaisiin myös energiahuoltoon.

5.3.3 Auditoinnit ja sertifioinnit

Kuten luvuissa 4.1.1 ja 4.3 esitettiin, vaatimus *tietoturva-auditoinneista* tai tiettyjen *tietoturvasertifikaattien* hankkimisesta voisi olla hyvin potentiaalinen keino parantaa myös sähköverkonhaltijoiden kyberturvallisuutta. Auditointien avulla organisaation tekniset tietojärjestelmät sekä organisatoriset menettelyt pystyttäisiin arvioimaan, ja tämän perusteella toimijan kyberturvallisuuden tasosta ja velvoitteiden noudattamisesta saataisiin selkeämpi kuva. Liikenne- ja viestintäministeriö on raportissaan Tietoturvan ja tietosuojan parantamisesta yhteiskunnan kriittisillä toimialoilla korostanut, että etenkin *ulkopuolisten arviointilaitosten* suorittamat auditoinnit voisivat lisätä organisaatioiden kyberturvallisuutta huomattavasti.[156]

Suoritetun auditoinnin perusteella kriittiselle toimijalle voitaisiin myöntää jonkin yleisesti tunnustetun *standardin* mukainen *tietoturvasertifikaatti*, joka toimisi todistuksena kyberturvallisuuden asianmukaisesta huomioimisesta organisaatiossa. Liikenne- ja viestintäministeriön raportin pohjalta annetussa valtioneuvoston periaatepäätöksessä esitetäänkin toimenpiteitä, joilla kriittiset toimijat velvoitettaisiin säännöllisesti auditoimaan niiden kriittiset tietoliikennetekniset prosessit ja toiminnot. Lisäksi merkittävimmät kriittiset toimijat velvoitettaisiin hankkimaan *ISO 27001-sertifikaatti* tai sitä vastaava tietoturvasertifikaatti vuoden 2025 loppuun mennessä.[157] Juuri sähköverkonhaltijat organisaatioina, jotka hyödyntävät toiminnassaan paljon teollisuusautomaatiota, voisivat korostuneesti hyötyä tiettyjen tietoturvastandardien noudattamisesta.[158]

---

[155] Liikenne- ja viestintäministeriö 2021, s. 37.

[156] Liikenne- ja viestintäministeriö 2021, s. 43.

[157] Valtioneuvosto 2021, s. 7–8.

[158] Pöyhönen 2018, s. 15.

Nykyisiin tietoturvasertifikaatteihin on kuitenkin hyvä suhtautua myös kriittisesti. Kyberturvallisuussääntelyä käsittelevässä kirjallisuudessa on esimerkiksi tuotu esille, että monet nykyisin käytössä olevat tietoturvastandardit perustuvat käytännössä melko yleisluonteisiin arviointikehyksiin, joten niiden teknisessä yksityiskohtaisuudessa vaikuttaisi olevan parantamisen varaa.[159]

Kuten luvuissa 4.1.1 ja 4.3 tuotiin esille, joiltakin muilta kriittisiltä toimialoita löytyy jo nykyisellään auditointeihin ja sertifiointeihin liittyvää sääntelyä. Myös sähkömarkkinalakiin voitaisiin harkita uutta pykälää, jossa sähköverkonhaltijat velvoitettaisiin teettämään säännöllisesti ulkopuoliset auditoinnit järjestelmiensä kyberturvallisuuden tasosta. Samassa yhteydessä voitaisiin säätää Energiaviraston valtuudesta antaa tarkempia määräyksiä näistä auditoinneista. Mallia voitaisiin ottaa esimerkiksi *vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain* 4 luvusta.

Samalla logiikalla sähkömarkkinalakiin voitaisiin harkita myös uutta pykälää sähköverkonhaltijoiden tietojärjestelmien vaatimustenmukaisuuden osoittamisesta tietoturvasertifikaatilla, samaan tapaan kuin on säädetty *sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain* 35 §:ssä.

Auditointi- ja sertifiointivelvoitteita olisi kuitenkin harkittava hyvin tarkkaan, sillä auditointien teettäminen tai sertifiointien hankkiminen voi tulla organisaatiolle hyvin kalliiksi. Esimerkiksi ISO 27001-sertifikaatin hankkiminen tuli erään tutkimuksen mukaan maksamaan pienelle ohjelmistoalan yritykselle kolmen vuoden aikana arviolta 76 480 euroa.[160] Kustannukset toki vaihtelevat organisaation toimialan, koon ja järjestelmien monimutkaisuuden mukaan. On kuitenkin mahdollista, että vaatimus sertifikaatin hankkimisesta tulisi joillekin pienemmille toimijoille kohtuuttoman kalliiksi.[161] Mikäli siis sähkömarkkinalakiin haluttaisiin lisätä vaatimuksia tietoturva-auditoinneista ja -sertifioinneista, olisi näiden vaatimusten soveltamisalaa harkittava hyvin tarkasti.

---

[159] Wong 2018, s. 103.

[160] Iivanainen 2019, s. 34.

[161] Liikenne- ja viestintäministeriö 2021, s. 55–56.

6 Yhteenveto

Sähköverkkojen toiminta ja turvallisuus on elintärkeää kaikille kriittisille ja myös vähemmän kriittisille toimijoille yhteiskunnassamme. Kriittiset toimijat nojaavat toiminnassaan yhä enemmän digitaalisiin tietojärjestelmiin ja viestintäverkkoihin, ja yhteiskunnan digitalisoituessa näiden toimijoiden kyberturvallisuudesta huolehtiminen on tullut entistä tärkeämmäksi.

Sähköverkonhaltijoiden kohdalla tämä tarkoittaa sitä, että toimijoiden olisi varmistettava sähköverkkojensa hallintaan käytettävien tietojärjestelmien ja -verkkojen turvallisuus, jotta haitalliset kyberhyökkäykset saataisiin estettyä. Mikäli hyökkäys asianmukaisista suojaustoimenpiteistä huolimatta tapahtuu, sähköverkonhaltijoiden olisi oltava valmiita raportoimaan selkkauksesta valvovalle viranomaiselle ja muille asiaankuuluville tahoille. Lisäksi sähköverkonhaltijoiden olisi pyrittävä parhaansa mukaan palauttamaan järjestelmiensä toimintakyky ja turvallisuus.

Onkin siis tärkeää, että lainsäädännöstämme löytyy asianmukaiset ja tarpeeksi kattavat säännökset, joilla sähköverkonhaltijat velvoitetaan huolehtimaan organisaationsa kyberturvallisuudesta. Tässä tutkielmassa selvitettiin sähköverkkojen kyberturvallisuussääntelyä ja tutkimuskysymykset kuuluivat seuraavanlaisesti:

1. Miten sähköverkkojen kyberturvallisuutta säännellään?

2. Miten muiden kriittisten toimialojen kyberturvallisuutta säännellään?

3. Miten sähköverkonhaltijoihin kohdistuvaa kyberturvallisuussääntelyä tulisi kehittää, jotta kyberuhkiin pystyttäisiin varautumaan paremmin?

Sähköverkkojen kyberturvallisuutta säännellään tällä hetkellä EU-tasolla, kansallisen lain tasolla sekä Energiaviraston laatimilla ohjeilla. Euroopan unionin säädöksistä merkittävin on *verkko- ja tietoturvadirektiivi (NIS-direktiivi)*, jossa asetetaan kyberturvallisuuden vähimmäisvaatimukset monille kriittisille toimijoille, muun muassa sähköverkonhaltijoille. Direktiivi on juuri päivitetty, ja uusi NIS2 -direktiivi tulee lähivuosina parantamaan kaikkien kriittisten toimialojen kyberturvallisuutta.

Merkittävimpinä säännöksinä NIS-direktiivissä esitetään 1) kyberturvallisuusriskien hallinnan vähimmäisvaatimukset sekä 2) vaatimus ilmoittaa kyberturvallisuuden poikkeamista

toimivaltaiselle kansalliselle viranomaiselle. Tämän tutkimuksen perusteella on todettu, että kyseiset säännökset ovat muotoiluiltaan hyvin yleisluonteisia, mistä johtuen jäsenvaltioille on jäänyt merkittävä valta ja vastuu säätää tarkemmista kyberturvallisuusvelvoitteista direktiivin implementoinnin yhteydessä.

Direktiivin velvoitteet on pantu kansallisesti täytäntöön *sähkömarkkinalailla*, josta löytyvät kyberturvallisuusriskien hallintaan, poikkeamista raportoimiseen ja varautumissuunnitteluun liittyvät säännökset. Lainopillisen analyysin perusteella tutkielmassa on päädytty siihen lopputulokseen, että nämä säännökset eivät ole riittävän täsmällisiä ja kattavia, jotta sähköverkonhaltijat olisivat lain tasolla velvoitettuja tehokkaisiin toimenpiteisiin kyberturvallisuudesta huolehtimiseksi. Lisäksi tutkielmassa on tuotu ilmi, että Energiavirastolla ei ole tällä hetkellä oikeutta antaa sitovia tarkentavia *määräyksiä* vaadittavista toimista.

Sähkö- ja maakaasumarkkinoiden valvonnasta annetussa laissa säädetään Energiaviraston valvontatoimivaltuuksista sekä oikeudesta hallinnollisiin sanktioihin. Tutkielmassa esitetyn selvityksen perusteella on osittain epäselvää, onko Energiavirastolla tällä hetkellä lakiperusteisia ja toimivia valtuuksia valvoa nimenomaan kyberturvallisuusvelvoitteiden noudattamista. Lisäksi Energiavirastolla ei vaikuta olevan nykyisellään mahdollisuutta määrätä sähköverkonhaltijoille tehokkaita sanktioita velvoitteiden noudattamatta jättämisestä. Tästä esimerkkinä on lain 16 §:n mukainen *seuraamusmaksu*, joka voidaan määrätä useidenkin sähkömarkkinalain pykälien vastaisesta menettelystä, mutta juuri kyberturvallisuusvelvoitteisiin liittyvät pykälät eivät kuulu säännöksen soveltamisalaan.

Tutkimuksessa on myös esitetty moniin viranomaislähteisiin vedoten, että itsessään epäselvä ja heikosti velvoittava kyberturvallisuuden velvoitesääntely aiheuttaa sen, että Energiaviraston voi olla valvontatilanteessa käytännössä hyvin vaikea osoittaa velvoitteiden laiminlyömistä. Lisäksi viranomaisten nykyiset resurssit eivät mahdollista velvoitteiden tehokasta valvontaa. Näin ollen vallitseva tilanne vaikuttaakin olevan se, että asianmukaisten teknisten ja organisatoristen kyberturvallisuustoimenpiteiden toteutus on jäänyt sähköverkonhaltijoiden oman aktiivisuuden varaan.

Tutkielmassa on osoitettu, että kyberturvallisuussääntelyn taso vaihtelee huomattavasti eri toimialoilla. Kriittisistä toimialoista parhaiten säänneltyjä ovat *digitaalinen infrastruktuuri*, *finanssimarkkinat* sekä *terveydenhuoltoala*. Tästä syystä tutkielmassa perehdyttiin juuri

näiden toimialojen sääntelyyn ja saatiin selville, että niillä laintasoinen sääntely on selvästi yksityiskohtaisempaa ja kattavampaa kuin energiahuollossa. Kenties merkittävin tutkimuksessa tehty huomio oli se, että kaikkien kolmen alan lainsäädännöstä löytyy toimivaltaisen viranomaisen *määräyksenantovaltuus*, jota kaikki kyseisten alojen valvovat viranomaiset ovat myös aktiivisesti hyödyntäneet. Lakia tarkentavat, sitovat määräykset tekevätkin näiden alojen sääntelystä merkittävästi yksityiskohtaisempaa ja velvoittavampaa, mikä näkyy myös tutkimusten perusteella näiden alojen parempana kyberturvallisuuden tasona.

Täsmällisen kyberturvallisuussääntelyn laatiminen etenkin laintasolle on hyvin hankalaa, sillä kybermaailma on jatkuvassa muutoksessa. Eduskuntatasoisen lainsäädännön päivittäminen on työlästä ja aikavievää, mistä johtuen yksityiskohtainen laintasoinen kyberturvallisuussääntely olisi vaarassa vanhentua nopeasti. Lisäksi tietyn alan kyberturvallisuussääntely koskettaa aina suurta joukkoa erilaisia toimijoita, jotka voivat erota huomattavastikin esimerkiksi kokonsa, toimintatyylinsä, organisaationsa rakenteen sekä kyberturvallisuustoimiin käytettävissä olevien resurssien puitteissa. Näin ollen laintasoisen kyberturvallisuussääntelyn on oltava myös tulevaisuudessa jossain määrin yleisluonteista.

Tästäkin huolimatta on tutkielmassa esitetyn selvityksen perusteella kuitenkin selvää, että sähköverkkojen laintasoista kyberturvallisuussääntelyä on varaa kehittää nykyistä yksityiskohtaisemmaksi ja velvoittavammaksi.

Juuri julkaistu *EU:n uusi kyberturvallisuusdirektiivi (NIS2 -direktiivi)* tullee lähivuosina monilta osin vastaamaan sääntelyn kehitystarpeisiin myös sähköverkkojen alalla, mikä on erittäin hyvä kehityssuunta kohti entistä resilientimpää kriittistä infrastruktuuria.

Lisäksi tässä tutkielmassa on annettu esimerkkejä tarkemmista parannusehdotuksista *sähkömarkkinalakiin* sekä *sähkö- ja maakaasumarkkinoiden valvonnasta annettuun lakiin*. Parannusehdotukset koskevat kyberturvallisuuden kattavampaa ja yksityiskohtaisempaa huomioimista sähköverkkojen kehitystyössä, velvollisuutta säännöllisten tietoturva-auditointien teettämiseen, velvollisuutta yleisesti tunnustettujen tietoturvasertifikaattien hankkimiseen, selkeää velvoitetta dokumentoida kyberturvallisuuden hallintatoimenpiteet sekä velvoitetta erillisen kyberturvallisuusstrategian laatimiseen.

Lisäksi tutkimuksessa on esitetty, että Energiaviraston toimivaltuutta kyberturvallisuusvelvoitteiden noudattamisen valvontaan voitaisiin valvontalaissa selkeyttää,

minkä lisäksi myös esimerkiksi lain 16 §:n mukainen seuraamusmaksu voitaisiin ulottaa koskemaan myös kyberturvallisuusvelvoitteiden laiminlyömistilanteita.

Kaikkein merkittävimpänä parannusehdotuksena tutkimuksessa on esitetty, että sähkömarkkinalakiin lisättäisiin Energiavirastolle valtuus antaa tarkempia sitovia määräyksiä kyberturvallisuuden toimenpiteistä, samoin kun on jo tehty monilla muilla kriittisillä toimialoilla.

Niin sähköverkkojen, kuin muidenkin kriittisten toimialojen kyberturvallisuussääntelyssä riittää takuuvarmasti selvitettävää ja tutkittavaa myös tulevaisuudessa. Ymmärrys kyberturvallisuudesta ja sen merkityksestä koko yhteiskunnan toiminnalle ja turvallisuudelle tulee väistämättä tulevina vuosina kasvamaan. Tätä tutkimusta tehtäessä on käynyt selväksi, että etenkin kotimaista kyberturvallisuuteen keskittyvää oikeuskirjallisuutta on tällä hetkellä todella vähän. Tätä selittää varmasti suurimmilta osin digitalisaation nopea kehitys ja se, että kyberturvallisuuteen liittyvä sääntely ei ole pysynyt muuttuvan kyberympäristön ja uusien uhkien perässä.

Erityisesti EU:n uusi kyberturvallisuusdirektiivi tulee todennäköisesti aiheuttamaan lähivuosina merkittäviä muutoksia kansalliseen lainsäädäntöön. Kuten tässäkin tutkimuksessa on tuotu ilmi, aikaisemman EU-sääntelyn implementoiminen kansalliselle tasolle on ollut haastavaa. Siksi lähivuosien kyberturvallisuussääntelyyn liittyvässä oikeustieteellisessä tutkimuksessa voisi olla kiinnostavaa keskittyä esimerkiksi juuri NIS2 -direktiiviin ja sen aiheuttamiin muutoksiin kansallisessa sääntelyssämme. EU-tasolla on parhaillaan meneillään myös muita kyberturvallisuuden kannalta merkittäviä säädöshankkeita ja kaikkinensa vaikuttaa siltä, että alan sääntely ja sitä kautta siihen liittyvät tutkimusmahdollisuudet tulevat jatkossa lisääntymään. Myös esimerkiksi Euroopassa vallitseva geopoliittinen tilanne tulee varmasti omalta osaltaan vauhdittamaan yhteiskunnallista keskustelua kyberturvallisuuden merkityksestä.