Ville Lahti

LIIKENNEJÄRJESTELMÄN VERKKO- JA TIETOJÄRJESTELMIEN TURVALLISUUDEN SÄÄNTELY

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Lahti, Ville
Liikennejärjestelmän verkko- ja tietojärjestelmien turvallisuuden sääntely
Jyväskylän yliopisto, 2022, 93 s.
Kyberturvallisuus, pro gradu tutkielma
Ohjaaja: Siponen, Mikko

Kriittisen infrastruktuurin osana olevat organisaatiot tarjoavat yhteiskunnan keskeisiä palveluita. Näiden palveluiden tarjoamisen jatkuvuutta ja turvallisuutta varmistetaan Euroopan unionin verkko- ja tietojärjestelmien turvallisuusdirektiivillä (NIS), jota parhaillaan ollaan EU:ssa uudistamassa. NIS-direktiivin velvoitteet ovat olleet osa kansallista lainsäädäntöä vuodesta 2018 asti, mutta aiheeseen liittyvää oikeustieteellistä tutkimusta ei ole aikaisemmin Suomessa julkaistu. Tutkielmassa oikeustieteen lainopillista tutkimusmetodia hyödyntäen tulkitaan ja systematisoidaan verkko- ja tietojärjestelmien turvallisuussääntelyä liikennejärjestelmässä raide-, tie- ja vesiliikenteen näkökulmista. Tutkimuksen tarkoituksena on oikeudellisesta näkökulmasta selventää, keitä sääntely koskee, mitä sääntelyn kohteena olevilta vaaditaan ja miten sääntelyn noudattamista valvotaan. Sääntelyn soveltamisalan osalta havaittiin sääntelyn koskevan vakiintunutta käytäntöä laajempaa joukkoa yhteiskunnan keskeisten palveluiden tarjoajia. Sääntelyn kohteena olevien keskeisten palveluiden tarjoajien riskienhallinta- ja ilmoittamisvelvollisuuden osalta luotiin sääntelyn sisältöä selkeyttäviä määritelmiä. Kuitenkaan määritelmillä ei pystytty täysin poistamaan sääntelyn jättämää tulkinnanvaraisuutta. Verkko- ja tietojärjestelmien turvallisuusvelvoitteiden noudattamista liikennejärjestelmässä valvoo Liikenne- ja viestintävirasto Traficom. Valvovan viranomaisen valvontavelvollisuuksissa tunnistettiin puute, joka voi heikentää raideliikenteen kyberturvallisuuden valvontaa sekä poiketa NIS-direktiivin vähimmäisvaatimuksista. Valvonnan toimivaltuuksissa havaittiin merkittäviä eroavaisuuksia eri liikennemuotojen välillä, vaikka kaikissa liikennöintimuodoissa on kyse samankaltaisten velvoitteiden noudattamisen valvonnasta. NIS-direktiivi velvoittaa jäsenvaltioita säätämään direktiivin nojalla annettujen kansallisten säännösten rikkomiseen sovellettavista seuraamuksista, mutta ainoastaan raideliikenteessä huomautuksesta ja varoituksesta seuraamuksena on säädetty. Kansallisessa lainsäädännössä Liikenne- ja viestintävirastolle on annettu määräystoimivaltaa. Vaikka määräystoimivalta ei kata kaikkia tutkielmassa tunnistettuja tulkinnanvaraisia tilanteita, tutkielmassa suositetaan määräystoimivallan hyödyntämistä ja esitetään mistä määräämällä sääntelyä voisi täsmentää.

Asiasanat: Verkko- ja tietojärjestelmäturvallisuus, kyberturvallisuus, NIS-direktiivi, liikennejärjestelmä, raideliikenne, meriliikenne, tieliikenne

ABSTRACT

Lahti, Ville
Network and information security regulation of the transport system
University of Jyväskylä, 2022, 93 pp.
Cyber Security, Master's Thesis
Supervisor: Siponen, Mikko

Organizations as part of the critical infrastructure provide essential services for society. Continuity and security of these services are ensured by security of network and information systems directive (NIS), which is planned to be replaced in European Union by new directive on high common level of cybersecurity. Obligations stemming from NIS-directive have been part of Finland's national legislation since 2018, but jurisprudential research has not been conducted before on this topic. Using legal dogmatic research method, the national network and information security legislation is interpreted and systematized *de lege lata* in transportation system (rail, road and maritime). The aim of the research is, from jurisprudential perspective, to clarify who are providers of essential services, what obligations these providers have and how the compliance of network and information security obligations are supervised. The study points out that national legislation obliges larger number of providers of essential services than what is previously understood. The study provides definitions, which clarify ambiguity of risk management and reporting obligations of providers of essential services. However, proposed definitions do not solve all ambiguities. The supervision of the compliance of network and information security obligations is tasked for the Finnish Transport and Communications Agency Traficom. The study identifies a shortcoming in Traficom's supervision obligations, which might hinder the supervision of cybersecurity compliance in railway transportation and fall behind from obligations of the NIS-directive. Even though NIS-obligations are nearly identical in transport system, the study shows that competent authority's powers and means to assess the compliance of NIS-obligations widely vary between transportation sectors. According to the directive, member states shall lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to NIS-directive. However, only in railway transportation the competent authority may issue notifications and warnings as a penalty. The national legislation provides for Traficom the authority to issue regulations on cybersecurity requirements, but the competence does not cover all ambiguities identified in this study. Nevertheless, the study recommends to issue regulation and provides proposals what the regulation could cover.

Keywords: Network and information security, cybersecurity, NIS-directive, transport system, rail transport, maritime transport, road transport

TAULUKOT

SISÄLLYS

1 JOHDANTO

Euroopan parlamentin ja neuvoston direktiivissä toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (verkko- ja tietojärjestelmien turvallisuusdirektiivi, NIS-direktiivi) on kysymys yhteiskunnan kriittisten toimintojen tietoturvallisuuden parantamisesta ja tietoturvallisuuden rajat ylittävästä yhteistyöstä EU:n sisällä. Direktiivi pantiin Suomessa täytäntöön useilla sektorikohtaisilla lakimuutoksilla, jotka tulivat voimaan 9.5.2018 eli lakeja on sovellettu jo lähes neljän vuoden ajan. Voimassa olevan NIS-direktiivin keskeisenä ajatuksena on, että yhteiskunnan toiminnan kannalta kriittisten organisaatioiden tulisi *tunnistaa* oman toimintansa kannalta merkittävät tieto- ja viestintäjärjestelmät, *huolehtia* niiden riskienhallinnasta, *dokumentoida* riskienhallinta sekä *ilmoittaa* valvovalle viranomaiselle merkittävistä tietoturvapoikkeamista. Suomessa liikennejärjestelmän osalta sääntely kohdistuu useisiin toimijoihin. Raideliikenteessä sääntely kohdistuu Väylävirastoon valtion rataverkon haltijana sekä Fintraffic Raide Oy:öön raideliikenteen ohjauspalveluiden tuottajana. Vesiliikenteessä sääntely kohdistuu useisiin tärkeimpiin satamiin sekä Fintraffic Meriliikenteenohjaus Oy:öön alusliikenteen ohjauspalveluiden tuottajana. Tieliikenteessä sääntelyn kohteena on muun muassa Fintraffic Tie Oy tieliikenteen liikenteenohjaus- ja hallintapalveluiden tuottajana. Parhaillaan EU:ssa pyritään uudistamaan NIS-direktiiviä. Ensimmäinen luonnosversio ehdotukseksi uudesta verkko- ja tietojärjestelmien turvallisuusdirektiivistä (NIS2) julkaistiin joulukuussa 2020. (Euroopan komissio, 2020) Loppuvuodesta 2021 Euroopan parlamentti sekä komissio julkaisivat omat uudet luonnosversiot NIS2-direktiivistä. (Euroopan komissio, 2021) Tämän tutkielman valmistuessa kevättalvella 2022 komissio ja parlamentti luonnostelevat yhdessä yhteistä ehdotusta NIS2 direktiiviksi. (EUR-lex, 2022)

NIS2-direktiiviuudistuksen taustalla olevan käsityksen mukaan nykyisellä voimassa olevalla NIS-sääntelyllä ei riittävissä määrin saavuteta tavoitetta eli yhteiskunnan keskeisten palveluiden saatavuuden turvaamista tietoturvallisuuden keinoin. Tämän johdosta tutkimuksen tekemisen aloittamista motivoi pohdinta, toimiiko NIS-sääntely tehokkaasti Suomessa sekä oletus, että nykyinen NIS-

sääntely toteuttaa heikosti sen tarkoituksen eli yhteiskunnan keskeisten toimialojen kyberturvallisuuden varmistamisen. Sääntelyn toimimattomuudelle voi löytyä useita selittäviä tekijöitä, joista yksi voi olla tiedon puute direktiivin ja kansallisen lainsäädännön sisällöstä. Tarkemmin jaoteltuna tiedon puute kansallisen verkko- ja tietojärjestelmien turvallisuussääntelyn sisällöstä voi johtua muun muassa direktiivin jättämästä tulkinnanvaraisuudesta, direktiivin vaikeaselkoisuudesta ja näiden tuloksena syntyvästä vaikealukuisuudesta. Vaikuttaisi siltä, että näitä direktiivitason heikkouksia ei ole täysin pystytty Suomessa korjaamaan saatettaessa direktiiviä osaksi kansallista lainsäädäntöä. Lisäksi vaikuttaisi siltä, että korkean kyberturvallisuuden tason tavoittelusta on tingitty sektorikohtaisten lakien soveltamisalaa määritettäessä. Edelleen kansallisella tasolla epätietoisuus lainsäädännön tarkasta sisällöstä on voinut vaikuttaa siihen, että valvovat viranomaiset eivät mahdollisesti ole selkeästi resursoineet valvontaa, valvontaa ei välttämättä ole tehty, eikä toisaalta sääntelystä selviä, tulisiko valvontaa ylipäänsä tehdä ennen merkittävän häiriön syntymistä. Lisäksi tutkimuksen taustalla on mahdollisuus, että raide-, vesi- ja tieliikenteen toimijat ovat mahdollisesti jättäneet ilmoittamatta tietoturvallisuuteen liittyvistä merkittävistä poikkeamista. Mahdollinen ilmoittamatta jättäminen voisi johtua siitä, että lainsäädännöstä ei helposti selviä, mitä merkittävällä poikkeamalla tarkoitetaan eli milloin heidän tulisi asiasta viranomaiselle ilmoittaa. Lainsäädäntö vaikuttaisi mahdollistavan toimivaltaisille viranomaisille mahdollisuuden antaa tarkempia määräyksiä siitä, mistä tietoturvapoikkeamista tulee ilmoittaa. Tällaisia sääntelyä selkeyttäviä määräyksiä ei kuitenkaan ole annettu. Toisaalta optimistisesti asiaan suhtautuen voi myös olla mahdollista, että raide-, vesi- ja tieliikenteen alueilla ei ole direktiivin kansallisen soveltamisen aikana eli lähes neljän aikana ollut tieturvallisuuden merkittäviä häiriöitä ja ne olisi kyetty käsittelemään, mikäli sellaisia olisi ollut. Tutkimuksen aloittamisen motiivin kytkeytyessä voimakkaasti direktiivin ja kansallisen lainsäädännön sisällön selvittämiseen, tutkimuksen tarkoitukseksi muodostui tavoite tulkita ja systematisoida voimassa olevan verkko- ja tietojärjestelmien turvallisuuslainsäädännön sisältöä. Sääntelyn nykytilaa tulkitsemalla ja systematisoimalla tutkimuksessa selvennetään, keitä sääntely ylipäänsä koskee, mitä sääntelyn kohteena olevilta vaaditaan ja kuinka vaatimusten noudattamista tulisi valvoa.

Voimassa olevan lainsäädännön sisällön tulkinta ja systematisointipyrkimys on erittäin ajankohtainen, koska mahdollinen NIS2-direktiiviuudistus luo tarpeen ja mahdollisuuden tarkastella voimassa olevaa sääntelyä ja kehittää sääntelyä toimivammaksi. NIS2-direktiiviluonnosten perustella vaikuttaisi siltä, että tulevaisuudessa sääntelyn piiriin voisi tulla uusia toimialoja, yksittäisiin toimijoihin kohdistuvat tietoturvavelvoitteet olisivat tarkkarajaisempia ja siten mahdollisesti vaatimustasoltaan korkeampia, minkä lisäksi viranomaisten toimivaltaan ja valvontavelvollisuuksiin tulisi mahdollisesti laajennuksia. Kokonaisuutena kiristyvä sääntely yhdistettynä oletukseen, että nykysääntely ei toimi, voisi merkitä sitä, että uudistuva sääntely aiheuttaisi sekä toimijoille että valvoville viranomaisille huomattavia lisäponnistuksia tietoturvallisuuden lisää-

miseksi. Vaadittava tietoturvallisuuden tason korotus ja korotuksen vaatimat resurssit olisivat mahdollisesti vähäisempiä ja helpommin toteutettavia, mikäli nykyisin voimassa oleva sääntely olisi selkeämpää sekä sitä sovellettaisiin ja valvottaisiin korkeaa tietoturvallisuuden tasoa tavoitellen.

1.1 Tavoitteet, tutkimuskysymys ja rajaukset

Tutkimus rakentuu lainsäädännön nykytilan selvittämisen varaan. Tutkimuskysymys on: *Kuinka tutkimuksen keinoin voimassa olevaa NIS-sääntelyä voidaan systematisoida ja tulkita?* Tutkimuskysymykseen vastaamista lähestytään analyyttisesti pilkkomalla pääkysymys edelleen pienemmiksi kysymyksiksi, joiden varaan tutkimuksen rakenne ja pääkysymykseen vastaaminen muodostuvat. Seuraavaksi esitellään samanaikaisesti tutkimuksen rakenne sekä tutkimuskysymykset pilkottuna.

Pääkysymykseen vastaaminen ensinnäkin edellyttää sääntelyn soveltamisalan selvittämistä eli vastaamista kysymykseen *mihin toimijoihin NIS-sääntelyä Suomessa raide-, vesi- ja tieliikenteen alalla sovelletaan*. Lisäksi soveltamisalaan liittyen selvitetään, vastaako toimijoiden määrittäminen direktiivin vähimmäistavoitetta ja tulisiko sääntelyn koskea laajempaa toimijajoukkoa direktiivin tarkoitus huomioiden. Näihin kysymyksiin vastattua siirrytään vastaamaan kysymykseen, *mitä sääntelyn kohteena olevilta toimijoilta kansallisen lainsäädännön mukaan vaaditaan*. Toimijoihin kohdistuvien vaatimusten osalta otetaan lähempään tarkasteluun erityisesti riskienhallinta ja ilmoittamisvelvollisuus. Osakysymykseen vastaaminen edellyttää tutkimuksessa selvitettävän, minkä tietoturvallisuudesta toimijoiden tulee varmistua, miten tietoturvallisuudesta tulisi varmistua ja onko olemassa jokin vähimmäisvaatimus, mikä toimijoiden tulisi täyttää. Riskienhallinnan osalta myös selvitetään, kuinka tarkasti toimijoiden tulisi dokumentoida riskienhallintansa. Tietoturvapoikkeamien ilmoittamisvelvollisuuden osalta tutkimuksessa selvitetään, mistä tietoturvapoikkeamista toimijoiden tulisi ilmoittaa. Ilmoitusvelvollisuutta koskevaan kysymykseen vastaaminen edellyttää, että selvitetään mitä tarkoitetaan merkittävällä tietoturvapoikkeamalla. Kansallisen lainsäädännön riskienhallinnan ja ilmoittamisvelvollisuuden kokonaisuuden käsittelyn lopuksi tutkimuksessa vastataan kysymykseen, vastaako kansallisessa lainsäädännössä asetetut vaatimukset direktiivin riskienhallinnan ja ilmoittamisvelvollisuuden vähimmäistavoitetta. Kun tutkimuksessa on selvitetty NIS-sääntelyn nykytilan osalta mihin toimijoihin velvollisuudet kohdistuvat ja mikä on velvollisuuksien sisältö, tutkimuksessa siirrytään selvittämään mahdollistaako NIS-sääntely tehokkaan ja tarkoituksenmukaisen viranomaisvalvonnan. Viranomaisvalvontaa koskevan kysymyksenasetteluun vastauksen antamista varten tutkitaan, *minkälaisia valvontavelvollisuuksia viranomaisilla on ja minkälaisia toimivaltuuksia valvonnan toteuttamiseksi viranomaisille on säädetty*. Valvontavelvollisuuksien ja toimivaltuuksien tutkimisen yhteydessä myös käsitellään, minkälaisia toimintavaihtoja viranomaisella on käytettävissä, mikäli NIS-sääntelyn noudattamisessa havaitaan puutteita. Toimintavaihtoehtojen selvittämisen lopuksi

tutkimuksessa vastataan, mahdollistaako lainsäädäntö hallinnollisen pakon tai sanktioiden käytön sekä minkälaista määräystoimivaltaa valvoville viranomaisille on annettu. Määräystoimivallan osalta edelleen vastataan, tulisiko toimivaltaisten viranomaisten hyödyntää määräystoimivaltaa sääntelyn selkeyttämiseksi ja mistä viranomaisten voisi olla hyvä määrätä sääntelyn nykytilan selkeyttämiseksi. Tutkimuksen viimeinen kappale on yhteenveto ja johtopäätökset. Yhteenvedossa tuodaan tiivistäen esille keskeisimmät havainnot, kuinka tutkimuksen keinoin lainsäädännön nykytilaa voidaan selkeyttää ja systematisoida sekä minkälaisia havaintoja voimassa olevan sääntelyn suhteesta NIS-direktiivin vähimmäisvaatimuksiin on tehty. Johtopäätöksissä tuodaan esille, mikä merkitys tutkimuksella on kansallisen verkko- ja tietojärjestelmien turvasääntelyn tulkintaan ja soveltamiseen sekä mitä mahdollisesti tulevan NIS2 sääntelyn osalta tulisi erityisesti huomioida.

Tutkimuksen kohteen eli oikeudellisen sääntelyn näkökulmasta tutkimus rajataan koskemaan voimassa olevaa EU:n NIS-direktiiviä sekä lakeja, joilla direktiivi on liikennejärjestelmässä laitettu täytäntöön. Näitä kansallisia lakeja ovat raideliikennelaki, alusliikennepalvelulaki, laki eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta (turvatoimilaki) sekä laki liikenteen palveluista. NIS-direktiivin sisällön osalta tutkimuksen ulkopuolelle rajataan esimerkiksi EU:n jäsenvaltioiden välisen tietoturvayhteistyön järjestäminen, kansalliset kyberturvallisuusstrategiat sekä digitaalisten palveluiden tarjoaminen. Verkko- ja tietojärjestelmien turvallisuussääntelyn tarkoituksena on tietoturvallisuuden keinoin varmistua yhteiskunnan keskeisten palveluiden saatavuudesta. Sääntelyllä on tiivis kytkentä valmius- ja varautumisasioihin sekä huoltovarmuuteen, mutta edellä mainittuihin liittyviä näkökulmia käsitellään vain siltä osin, kun ne tukevat verkko- ja tietojärjestelmien turvallisuussääntelyn ymmärtämistä. Verkko- ja tietojärjestelmien turvallisuussääntely ei ole syntynyt pelkästään samaan aikaan EU:n tietosuoja-asetuksen kanssa, vaan niillä on myös läheinen kytkös toisiinsa. Verkko- ja tietojärjestelmäturvallisuuden sekä tietosuojasääntelyn rajapintaa tutkimuksessa käsitellään vain siinä yhteydessä, kun kysymys on riskienhallinta- ja ilmoittamisvelvollisuuksien sisällön tulkinnasta ja vertailuista. NIS-direktiivin perusteella tehdyt muutokset liikenteen sektorikohtaiseen lainsäädäntöön eivät ole ainoita kansallisia tietoturvasäännöksiä. Erityisesti milloin NIS-sääntelyn kohteena oleva toimija on viranomainen, viranomaiseen kohdistuu myös muista laeista kansallisia tietoturvallisuusvaatimuksia. Kuitenkin tämä muu kansallinen tietoturvasääntely rajataan tutkimuksen ulkopuolelle. Sääntelyn soveltamisalan näkökulmasta tutkimus rajataan koskemaan liikennejärjestelmää ja liikennejärjestelmän osalta edelleen vain raide-, vesi- ja tieliikennettä. Ilmailu eli lentoliikenne on erittäin tärkeä osa liikennejärjestelmää, mutta se rajataan tutkimuksen ulkopuolelle. Rajauksen perusteena on, että, ilmailun sisäinen tietoturvasääntely vaikuttaa kehittyvän muita liikennemuotoja nopeammin ja NIS2-direktiiviehdotuksessa ilmailun sektorikohtaiselle erityissääntelylle mahdollisesti annetaan etusija suhteessa NIS2-direktiiviin. Liikennejärjestelmään kohdistuva rajaus myös helpottaa nykysääntelyn tutkimusta viran-

omaisten toimivaltuuksien näkökulmasta, koska liikennejärjestelmän osalta Liikenne- ja viestintävirasto Traficom on toimivaltainen valvontaviranomainen. Vaikka ilmailu ja muut NIS-direktiivissä mainitut toimialat ovat rajattu tutkimuksen ulkopuolelle, tutkimuksen tulokset voivat olla tapauskohtaisesti yleistettävissä niin ilmailun kuin myös muille NIS-toimialoille kuten energiaan, juomaveteen tai terveydenhuoltoon.

1.2 Tutkimusmetodi

Tutkielmassa käytetään lainopillista tutkimusmetodia verkko- ja tietojärjestelmien turvallisuussääntelyn nykytilan selvittämiseksi. Kolehmaisen (2015, s. 107) mukaan Siltala (2003) määrittelee oikeustieteen tiedonintresseiksi muun massa laintulkinnan, systematisoinnin, sääntelyn vaikutusten arvioinnin ja sääntelyn kehittämisen. Tässä tutkimuksessa tiedonintressini on voimassa olevan NIS-sääntelyn osalta tulkita ja systematisoida voimassa olevan oikeuden sisältöä.

Raimo Siltalaan viitaten Kolehmainen tiivistää, että lainoppi yleensä tuottaa kannanottoja siitä, mikä on voimassa olevan oikeuden tietynhetkinen sisältö vallitsevan lainopin mukaisesti eli tiedonintressinä on, mitä oikeus on. (Kolehmainen, 2015) Tutkimuksessa verkko- ja tietojärjestelmien turvallisuussääntelyä tutkitaan lainopin eli oikeusdogmatiikan menetelmin hyödyntäen erityisesti lainsäädännön sanamuodon mukaista tulkintaa ja tulkiten lainsäädännön tarkoitusta. Tutkimuksessa nojaudutaan Aulis Aarnion ja Aleksander Peczenikin kehittämään oikeuslähdeoppiin, kun eri oikeuslähteitä käytetään oikeudellisessa argumentaatiossa. (Ks. Kolehmainen, 2015, s. 116-117 Aulis Aarnion ja Aleksander Peczenikin oikeuslähdeopista)

Tutkimuksessa arvioidaan kansallisen verkko- ja tietojärjestelmien turvallisuussääntelyn suhdetta NIS-direktiivin vähimmäistasoon, jolloin EU-oikeuden tulkintaperiaatteet korostuvat. NIS-direktiivin sisältöä ja tarpeellisin osin EU-oikeutta laajemmin tulkitessa tutkimuksessa sovelletaan ensisijaisesti sanamuodonmukaista tulkintaa, mutta tarvittaessa hyödynnetään systemaattista tulkintaa sekä lisävälineenä valmisteluasiakirjoja siltä osin kuin se on mahdollista. Taluksen ja Penttisen (2015) mukaan EU:n perussopimuksissa ei määrätä, että EU-oikeuden tulkintametodeilla olisi tietty etusijajärjestys. Lähtökohtaisesti EU-oikeutta tulkitaan sanamuodon mukaisesti. Sanamuodon mukaisen tulkinnan lisäksi systemaattinen tulkintaa voidaan soveltaa eli tulkinnassa EU-oikeuden normit on sijoittava asiayhteyksiinsä ja tulkinnassa on huomioitava EU-oikeus kokonaisuudessaan. Lisäksi EU-tuomioistuin on ratkaisukäytännössään nojautunut teleologiseen tulkintaan eli pyrkinyt toteuttamaan säännöksen tarkoitusta, koska se mahdollistaa normien tarkoituksen toteutumisen muuttuvassa ympäristössä. Lisäksi lisääntyvä avoimuus EU-oikeuden esitöistä mahdollistaa uudenlaisia EU-oikeuden tulkintamahdollisuuksia, joita voidaan hyödyntää lisävälineinä EU-sääntelyn sanamuodon, asiayhteyden ja tavoitteiden selventämiseksi. (Talus & Penttinen, 2015)

1.3 Kirjallisuuskatsaus

Jonna Rantala (2017) selvitti pro gradu tutkielmassa, mitä riskejä NIS-direktiivi tuo yrityksille, mitä direktiivi tuo yritysten riskienhallintaan ja mihin toimijoihin direktiiviä sovelletaan. (Rantala, 2017, s. 2) Rantala korosti, että kyseessä ei ole oikeustieteellinen tutkimus, vaan sääntelyä tarkasteltiin ylätasolla kokonaiskuvaa luoden. Rantalan mukaan suurin direktiivin tuoma riski toimijoille oli compliance-riski, minkä lisäksi tutkimuksessa tuodaan esiin strategisia ja operatiivisia riskejä. Compliance-riskeistä suurimmaksi arvioitiin, että toimija ei täytä lain vaatimuksia, jolloin toimija joutuu mukautumaan lakiin sen noudattamiseksi ja negatiivisten seurausten minimoimiseksi. Compliance-riskin osa-alueiksi tunnistettiin sääntelyn tulkinnanvaraisuus velvoitteiden epäselvyyden sekä sääntelyn soveltamisalaan kuuluvien toimijoiden määrittelyn näkökulmista. (Rantala, 2017, ss. 34-37) Strategisena riskinä tunnistettiin muun muassa toimijaan kohdistuvien vaatimusten tulkinnanvaraisuudesta johtuvat yli- tai ali-investoinnit tai jopa passiivisuus. (Rantala, 2017, s. 39) Operatiivisena riskeinä tunnistettiin muun muassa toimijan liikesalaisuuksien paljastuminen viranomaisten epäonnistuessa suojaamaan niitä sekä riski, että turvallisuusohjeet luodaan ainoastaan sen takia, että direktiivi vaatii, eivätkä vastaa toimijan todellisia tarpeita. (Rantala, 2017, s. 41)

Liikenne- ja viestintäministeriön (LVM) verkko- ja tietojärjestelmien turvallisuusdirektiivin täytäntöönpanoa tukevan työryhmän loppuraportissa kansalliseksi tavoitteeksi esitettiin turvattavan yritysten tietoturvariskien hallinta osana muiden liiketoiminnan riskien hallintaa. Työryhmä esitti direktiivin velvoitteiden täytäntöönpanoa osana sektorikohtaista sääntelyä, ettei päällekkäisiä muusta lainsäädännöstä johtuvia velvollisuuksia tarpeettomasti syntyisi. (LVM, 2017, s. 29) Työryhmän käsityksen mukaan direktiivi velvoittaa jäsenvaltioita tekemään luettelon keskeisistä palveluista ja myös määritettävä, mihin toimijoihin direktiivin vaatimuksia sovelletaan. (LVM, 2017, s. 9 ja 33) Työryhmä kuitenkin katsoi, että tarkoituksenmukaisinta on määrittää lainsäädännöllisin kriteerein (LVM, 2017, s. 34), minkä voi ymmärtää tarkoittavan, että soveltamisalan piiriin kuuluvat nimettäisiin tai määritetäisiin sektorikohtaisissa laeissa. Työryhmä totesi, että tuolloin voimassa ollut tietoturvasääntely oli hajanaista ja oli epäselvää, pysyitkö tuolloin voimassa olleiden riskienhallintavelvoitteiden sanamuodonmukaisesta tulkinnasta tekemään johtopäätöksen, että riskienhallinta koskisi myös tietoturvavelvoitteita. (LVM, 2017, s. 29) Työryhmä ei ottanut kantaa, kuinka ilmoitusvelvollisuuteen kuuluvat merkittävät tietoturvapoikkeamat määriteltäisiin, mutta esitti, että lainsäädäntöä tulisi täydentää verkko- ja tietojärjestelmien riskienhallintaan ja turvallisuuspoikkeamailmoituksiin liittyen. (LVM, 2017, s. 34) Raportin lopuksi työryhmä totesi korkean verkko- ja tietojärjestelmien turvallisuuden varmistamisen vähimmäisvelvoitteista, että "direktiivin luonteesta johtuen ei kuitenkaan ole täysin selvää, mitä on pidettävä vähimmäisvelvoitteina”. (LVM, 2017, s. 35)

Antti-Ilari Söderholm (2018) pro gradu tutkimuksessa kuvaili kyberturvallisuuteen kohdistuvia uhkia, NIS-direktiivin sisältöä ja kyberturvallisuusyhteistyötä. Söderholmin keskeinen havainto oli, että kyberturvallisuusyhteistyössä EU:n sisällä on paljon haasteita ja kehitettävää erityisesti luottamuksen näkökulmasta. Söderholm toi esille, että olisi syytä arvioida tietoteknisten laitteistojen (hardware) ja ohjelmistojen valmistajien saattaminen NIS-sääntelyn piiriin, koska valmistajat ovat merkittävä tekijä kyberturvallisuuden kokonaisuudessa. Tutkimuksen rajauksissa Söderholm korosti, että kyseessä ei ole oikeudellinen tutkimus NIS-direktiivistä eikä NIS-direktiiviä arvioida oikeudellisesta näkökulmasta. Söderholm tunnisti tutkimuksessaan, että erityisesti NIS-sääntelyn kansallisesta toimeenpanosta ja oikeudellisesta näkökulmasta tehtävä tutkimus olisi tarpeen. (Söderholm, 2018, s. 82)

Jouni Pöyhösen väitöskirjassa NIS-direktiiviä sivuttiin direktiivin kattamien eri sektoreiden osalta. Pöyhönen korosti NIS-direktiivin kansallisen täytäntöönpanon vaikutuksia Liikenne- ja viestintäviraston sekä erityisesti Kyberturvallisuuskeskuksen tilannekuvan ja kokonaistilannetietoisuuden parantumisen näkökulmasta. (Pöyhönen, 2020, s. 90-92)

Lauri Alhamon (2021) opinnäytteessä "Kone- ja tietoturvallisuus - Riskien arvioinnin suhteet ja laillinen viitekehys" tutkimuskysymyksinä olivat, miten tietoturvauhat tulee ottaa huomioon koneiden riskien arvioinnissa, miten lainsäädännön vaatimuksiin vastataan, miten vaarat tunnistetaan ja mitkä asiat vaikuttavat tietoturvariskin suuruuteen ja merkittävyyteen. (Alhamo, 2021, s. 7) Tutkimuksen lopputuloksena syntyi kuvaus koneiden tietoturvavaatimuksiin liittyvää viitekehystä, hahmotelma tietoturvariskien arvioinnin toimintakuvauksen sekä Etteplan Oy:lle luotiin näköispainoksen koneiden tietoturvallisuuden esiarviointityökalusta. (Alhamo, 2021, s. 2) Alhamo tunnisti oleelliseksi mahdollisen NIS2 direktiivin soveltamisalan laajentumisen koneiden valmistajien suuntaan, minkä lisäksi EU:n asetusluonnos konetuotteista tulee mahdollisesti sisältämään tarkempia tietoturvavelvoitteita. (Alhamo, 2021, ss. 29-31) Alhamon tutkimuksessa lainsäädäntöä ja standardeja käsiteltiin ylätasolla konetekniikan näkökulmasta eikä niinkään oikeustieteen tai tietotekniikan näkökulmasta. (Alhamo, 2021, s. 9)

Mikko Soikkelin (2021) pro gradu tutkielmassa NIS-direktiivin pohjalta annetun sektorikohtaisen lainsäädännön tunnistettiin sisältävän velvoitteita ja eri hallinnonaloille kohdistettuja valvontavastuita, mutta niiden sisältöä ei käsitelty tarkemmin. (Soikkeli, 2021, ss. 37-38)

LVM:n Digirata-valmisteluvaiheen loppuraportissa todettiin kyberturvallisuusriskienhallinnan rautatieympäristössä olevan vasta alkuvaiheessa ja rautateiden kyberturvallisuutta koskevan sääntelyn kehittämisen aloitetun EU-jäsenvaltioissa eri tavoin NIS-direktiivin myötä. (Pylvänäinen ym., 2021, s. 26)

LVM:n Liikenteen automaation lainsäädäntö- ja toimenpidesuunnitelmassa liikenteen automaation kyberturvallisuuteen liittyen korostetaan tietoturvan ja tietosuojan parantamista yhteiskunnan kriittisillä toimialoilla koskevan Valtioneuvoston periaatepäätöksen kirjausta: ”Tietoturvan tasoa ohjattaisiin nykyistä

tarkemmilla ja paremmin kohdennetuilla lakisääteisillä vaatimuksilla ja velvoitteilla, joiden toteutumista valvottaisiin aktiivisesti.” Raportin mukaan lakisääteisten vaatimusten ja velvoitteiden sekä valvonnan toteutuminen on yhteydessä NIS2-direktiiviuudistukseen. (Miettinen, Miettinen, Hauta, Töyrylä & Reinimäki, 2021, s. 74)

Porcedda tutki EU:n tietoturvasääntelyä e-Privacy, Framwork, eIDAS, NIS, GDPR ja PSD2 sääntelyitä vertaillen. Hän havaitsi, että tietoturvapoikkeama määritellään sääntelyssä samankaltaisesti ja kaikki säädökset sisälsivät riskiperusteisen tietoturvallisuuden hallintasäädöksen, jonka jälkeen säädöksissä asetettiin eritasoisia ilmoitusvelvollisuuksia kyberpoikkeamista. Ilmoitusvelvollisuuksien tarkoituksia tunnistettiin kolme erilaista, jotka kaikki toteutuvat NIS-direktiivissä samanaikaisesti: Toisilta oppiminen, yleisön tietoisuuden lisääminen ja oman toiminnan kehittäminen. Tutkimuksen mukaan yhdessäkään säädöksessä ei suoraan kerrota, kuinka riski tai vahingon määrä lasketaan. (Porcedda, 2018)

NIS-direktiivin, tietosuoja-asetuksen ja EU:n kyberturvallisuusviraston ENISA:n suhdetta käsittelevässä artikkelissa NIS-direktiivin merkitystä käsiteltiin EU-oikeuden tasolla ottamatta kantaa yksittäisten jäsenvaltioiden lainsäädäntöratkaisuihin. Artikkelin kirjoittajat tukeutuivat useissa kannanotoissaan NIS-yhteistyöryhmän julkaisuihin tulkitessaan NIS-direktiivin aukkokohtia. (Markopoulou, Papakonstantinou & de Hert, 2019)

NIS-direktiivin ja tietosuoja-asetuksen mukaisten ilmoittamisvelvollisuuksien aikamääreitä käsittelevässä artikkelissa tuotiin esille, että NIS-direktiivi tarjoaa vain abstraktin aikamääreen ilmoituksen tekemiselle, joskin esimerkiksi Isossa-Britanniassa ja Virossa on kansallisessa lainsäädännössä säädetty konkreettisista aikarajoista. (Schmitz-Berndt & Schiffner, 2021)

Oikeuskäytäntöä NIS-direktiiviin soveltamiseen liittyen ei ole tätä tutkimusta tehdessä löytynyt. Oikeuskäytäntöä on etsitty erityisestä Suomesta ja Euroopan unionin tuomioistuimen tasolta. Lisäksi muiden EU-jäsenvaltioiden NIS-direktiivin soveltamiseen liittyvää oikeuskäytäntöä on etsitty e-justice.europa.eu sivuston kansallisten oikeustapausten hakupalveluita hyödyntäen, mutta oikeuskäytäntöä ei ole löytynyt. Oikeuskäytännön puuttuminen merkitsee, että vahvasti velvoittavista oikeuslähteistä EU:n tuomioistuimen prejudikaatteja ei ole käytettävissä ja heikosti velvoittavista oikeuslähteistä käytössä on vain kansallinen lainvalmisteluaineisto.

Tämän tutkimuksen näkökulmasta neljä keskeistä suomalaista julkaisua eli Rantalan, Söderholmin ja Alhamon tutkimukset sekä LVM:n loppuraportti korostivat konkreettista tarvetta kyberturvallisuuden vaatimustenhallinnan oikeustieteelliselle tutkimukselle. Esimerkiksi Alhamon tutkimuksessa tunnistettiin koneiden tieturvallisuuteen liittyvää sääntelyä, mutta tutkimuksessa sääntelyn sisältö rajattiin tutkimuksen ulkopuolelle. Kun tutkimuksen kohteena on oikeudellinen sääntely, kyberturvallisuuden vaatimustenhallintaa on perusteltua tutkia oikeustieteelle tyypillisiä tutkimusmenetelmiä hyödyntäen. Vastaavasti LVM:n loppuraportin loppupäätelmä NIS-direktiivin vähimmäisvelvoitteiden epäselvyydestä vaikuttaa tätä tutkimusta tehdessä olevan edelleen pätevä. Tälle

tutkimukselle ei mahdollisesti olisi tarvetta, mikäli NIS-direktiiviä laadittaessa ja sen velvoitteita kansallisesti voimaan saatettaessa olisi pystytty luomaan selkeämpää sääntelyä.

2 VERKKO- JA TIETOJÄRJESTELMIEN TURVALLISUUSSÄÄNTELY LIIKENNEJÄRJESTELMÄSSÄ

NIS-direktiivin kaksi tärkeintä tavoitetta ovat varmistaa korkea kyberturvallisuuden taso kriittisillä toimialoilla ja luoda EU-jäsenvaltioiden välille tehokas yhteistyömekanismi tämän tavoitteen edistämiseksi. (DigitalEurope, 2016) NIS-direktiivin johdantokappaleen 44 mukaan korkean kyberturvallisuuden tason varmistamiseksi tulisi edistää riskienhallintakulttuuria, johon sisältyy riskiarviointi ja riskeihin suhteutettujen turvallisuustoimenpiteiden toteutuminen.

Ennen verkko- ja tietojärjestelmien turvallisuussääntelyn oikeudelliseen puoleen syventymistä on syytä nykytilan konkretisoimiseksi ensin lyhyesti perehtyä sääntelyn toimeenpanon näkyvimpään puoleen eli raportoituihin poikkeamiin ja niitä koskeviin tilastoihin. NIS-direktiivin mukaisesti perustetun yhteistyöryhmän (NIS Cooperation Group, NIS CG) 2021 raportin mukaan koko EU-alueella liikennesektorilla NIS-ilmoituksia tehtiin vuonna 2019 yhteensä 60 kappaletta, mikä on noin 14 % koko vuoden ilmoituksista. Vuonna 2020 liikennesektorin ilmoituksia kertyi yhteensä 44 kappaletta, mikä on noin 6 % kaikista vuoden ilmoituksista. Kokonaisilmoitusmäärät ovat nousseet 432 ilmoituksesta vuonna 2019 yhteensä 756 ilmoitukseen vuonna 2020. Noin 48 % tapauksien juurisyistä kategorisoidaan järjestelmävirheeksi, jonka taustalla on usein ohjelmointivirhe tai laitteistoin virheet (software bugs or hardware failures). Noin 41 % tapauksien juurisyistä johtui haitallisesta toiminnasta, jonka taustalla useimmiten oli haittaohjelma- tai kalasteluhyökkäys. (NIS CG, 2021, ss. 2-3 ja 9-10)

NIS yhteistyöryhmän mukaan vuoden 2019 loppuun mennessä suurin osa jäsenvaltioista oli saattanut NIS-direktiivin osaksi kansallista lainsäädäntöä. Tosin osa jäsenvaltioista oli vasta tunnistanut keskeiset toimijat ja määrittänyt ilmoituskynnykset. Raportissa tuotiin esille, että ilmoitusten sisältö vaihtelee paljon, koska ilmoituskriteerit ja kynnykset voivat vaihdella jäsenvaltioiden sekä myös yksittäisten sektoreiden väleillä. Raportissa ilmoitukset kategorisoidaan kuuteen eri tyyppiin. Suluissa kappalemäärä ja prosentuaaliset määrä vuoden 2020 EU-alueen ilmoituksista:

a) Poikkeama on aiheuttanut katkoksen keskeisessä palvelussa tai digitaalisessa palvelussa (saatavuus, 171 kpl, 23 %).
b) Poikkeama on muutoin vaikuttanut keskeisiin tai digitaalisiin palveluihin (luottamuksellisuus, eheys tai autenttisuus, 69 kpl, 9 %).
c) Poikkeaman vaikutukset ilmenevät keskeistä tai digitaalista palvelua tukevissa toiminnoissa kuten toimistoverkossa, joka on erillään tuotantojärjestelmästä (84 kpl, 11 %).
d) Uhka tai haavoittuvuus raportoitiin merkittävänä, mutta siitä ei aiheutunut välittömiä vaikutuksia (7 kpl, 1 %).
e) Poikkeama vaikutti palautumiseen, esimerkiksi varmuuskopiojärjestelmään tai varajärjestelmän automaattiseen käynnistymiseen (failover). (alle 1 %, tarkkaa lukua ei ilmoitettu)
f) Läheltä piti tilanne, jossa poikkeama ei aiheuttanut vaikutuksia esimerkiksi onnenkantamoisen tai tehokkaasti toteutettujen turvallisuustoimenpiteiden ansiosta. (37 kpl, 5 %) (NIS CG, 2021, s. 6)

2.1 Keskeisten palveluiden tarjoajat

Tässä liikennejärjestelmän keskeisten palvelun tarjoajia (operator of essential services) käsittelevässä kappaleessa selvitetään, mihin toimijoihin NIS-sääntelyä Suomessa raide-, meri- ja tieliikenteen alalla sovelletaan. Lisäksi soveltamisalaan liittyen selvitetään, vastaako palvelun tarjoajien määrittäminen direktiivin vähimmäistavoitetta ja tulisiko sääntelyn koskea laajempaa palvelun tarjoajien joukkoa direktiivin tarkoitus huomioiden. Näihin kysymyksiin vastataan tarkastelemalla ensin kaikkien keskeisten palvelujen määrittämisestä koskevia yleisiä säännöksiä, jotka ovat tarpeen liikennemuotokohtaisia alakappaleita käsiteltäessä. Yleisten säännösten tarkastelun jälkeen siirrytään liikennemuotokohtaisesti raide, vesi- ja tieliikenteen näkökulmista tarkastelemaan Suomen sektorikohtaista lainsäädäntöä keskeisten palvelujen määrittämisestä. Kappaleen lopuksi verrataan Suomen lainsäädäntöä NIS-direktiiviin ja arvioidaan tulisiko kansallisen sääntelyn koskea laajempaa palveluiden tarjoajien joukkoa direktiivin mukaisesti.

Käytännönläheisesti luonnehtien keskeisen palvelun tarjoajalla tarkoitetaan organisaatiota, joka tarjoaa yhteiskunnan elintärkeää toimintoa. Suomalaisessa keskustelussa tällaisista toimijoista saatetaan käyttää käsitteitä huoltovarmuuskriittinen, kokonaisturvallisuuden kannalta tärkeä tai kriittisen infrastruktuurin tarjoaja. Yhtä keskeisen palvelun tarjoajan määritelmää ei löydy Suomen lainsäädännöstä, koska Suomessa NIS-direktiivin velvoitteet on saatettu voimaan sektorikohtaisella sääntelyllä eli jokaista toimialaa koskevaan erityislainsäädäntöön on tehty tarvittavat lakimuutokset. Kuitenkin NIS-direktiivin kansallista täytäntöönpanoa koskevassa hallituksen esityksessä todetaan, että yhteiskunnan kannalta keskeiset toiminnot on määritelty yhteiskunnan tuvallisuusstrategiassa. (HE 192/2017 vp, s. 10) Tämän viittauksen voi katsoa antavan stra-

tegialle keskeisen merkityksen myös direktiivin soveltamisalaa arvioitaessa. Yhteiskunnan turvallisuusstrategiassa (YTS) liikennepalveluiden käytettävyyden ja saatavuuden varmistaminen on Liikenne- ja viestintäministeriön vastuulla. Tavoitteena on, että markkinaehtoisten, laadukkaiden, turvallisten ja toimintavarmojen liikennepalvelujen käytettävyys ja saatavuus varmistetaan niin häiriötilanteissa kuin poikkeusoloissa. Väestön toimeentulolle ja elinkeinoelämälle kriittiset kuljetukset ovat yksi keskeinen palvelu ja tämän takia varautumisvelvoite on sisällytetty muun muassa rautatieliikenteen harjoittajille ja metroliikenteen harjoittajalle. (Turvallisuuskomitea, 2017, s. 66) NIS-direktiivi saatettiin raideliikenteessä voimaan selkeästi YTS:n tunnistamaa tavoitetta suppeammin, vaikka YTS:n ja NIS-direktiivin kansallinen voimaansaattaminen ajoittuvat samaan ajankohtaan ja että YTS:ssa rautatieliikenteen harjoittajat ja metroliikenteen harjoittaja tunnistettiin yhteiskunnan turvallisuuden kannalta kriittisiksi.

Vaikka keskeisten palveluiden tarjoajien määritelmää ei lainsäädännöstä löydy, määritelmä on kuitenkin löydettävissä direktiivin täytäntöönpanoa koskevan hallituksen esityksen perusteluista ja direktiivin artikloista 5(2) ja 6. Määritelmä on kolmekohtainen:

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. (HE 192/2017 vp, s. 38)

Edellä mainituista kolmesta kriteeristä ensimmäinen, tarjoaako toimija yhteiskunnan toimintojen kannalta keskeistä palvelua, on direktiivin johdantokappaleen 20 ohjeistuksen mukaisesti suoraviivaisesti määritettävissä: "Arvioitaessa sitä, tarjoaako toimija yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeistä palvelua, on riittävää tarkastella, tarjoaako kyseinen toimija palvelua, joka sisältyy keskeisten palvelujen luetteloon." Keskeisten palveluiden luettelo on direktiivin liitteessä II. Liitteessä määritellään direktiivin soveltamisalan piiriin kuuluvat yhteiskunnan alat: Energia, liikenne, pankkiala, finanssimarkkinoiden infrastruktuuri, terveydenhuoltoala, juomaveden toimittaminen ja jakelu sekä digitaalinen infrastruktuuri. Liitteen kohdassa kaksi tarkennetaan liikennetoimialalta, mitkä ovat raide-, vesi- ja tieliikenteen keskeisiä toimijoita. Myös NIS-direktiivin koordinaatioryhmän ei sitovassa ohjeessa esitetään vastaava tulkinta (a) kohdan soveltamisesta. (NIS CG, 2018c, s. 7)

Toisena keskeisten palveluiden tarjoajien kriteerinä on, onko palvelun tarjonta riippuvainen verkko- tai tietojärjestelmistä. Verkko- ja tietojärjestelmien määritelmä löytyy NIS-direktiivin 4(1) artiklasta, mutta nykyaikana määritelmä ei tuottane tulkintaongelmia. Käytännössä verkko- ja tietojärjestelminä pidetään kaikkia järjestelmiä, joissa käsitellään digitaalista tietoa sekä kaikkia laitteita, jotka osallistuvat signaalin käsittelyyn. Lisäksi kriittisen palvelun tulee olla riippuvainen näistä järjestelmistä. Mikäli yhteiskunnassa on vielä sellaisia kriittisiä palveluja olemassa, jotka toimivat verkko- ja tietojärjestelmistä riippumatta,

nämä palvelut tulisi jättää määritelmän soveltamisalan ulkopuolelle. Selvyyden vuoksi on syytä todeta, että määritelmä ei edellytä kysymyksessä olevan julkisesti tunnettu tai internettiin kytketty verkko- tai tietojärjestelmä. Nykypäivänä lähtökohdaksi voitaneen ottaa, että käytännössä kaikki yhteiskunnan keskeiset toiminnot ovat tavalla tai toisella riippuvaisia verkko- tai tietojärjestelmien toiminnasta.

Kolmas keskeisten palveluiden tarjoajien määrittämisen kriteeri on haasteellisin ja tulkinnanvaraisin, minkä johdosta lopulta koko määrittelyssä kysymys on kokonaisharkinnasta. Jäljempänä esitettävän tulkinnanvaraisuuden johdosta on helppo yhtyä hallituksen esityksen toteamuksiin, että direktiivi jättää erittäin huomattavaa liikkumavaraa keskeisten toimijoiden määrittämiseen ja direktiivi jättää keskeisyyden arvioinnin jäsenvaltioiden harkintaan. (HE 192/2017 vp, ss. 44-45) Kolmannen kriteerin mukaan poikkeamalla palvelussa tulisi olla merkittäviä vaikutuksia palvelun tarjoamiseen. Seuraavaksi esitetään arviointikriteerejä, kuinka direktiivin käsitettä *merkittävä vaikutus palvelun tarjoamiseen* tulisi tulkita. Tässä yhteydessä on syytä pitää mielessä, että NIS-direktiivi on minimiharmonisoiva direktiivi eli EU:n jäsenvaltioiden tulee kansallisella sääntelyllä saavuttaa direktiivin vaatimusten vähimmäisvaatimukset, mutta jäsenvaltiot saavat ylittää direktiivin tavoitteet ja valita liikkumavaran mukaisesti keinot tavoitteiden saavuttamiseksi. Lisäksi on huomioitava, että keskeiseksi toimijaksi määritetyn organisaation tai yrityksen kaikki toiminnot eivät välttämättä ole, eikä niiden tarvitsekaan olla, yhteiskunnan toiminnan kannalta keskeisiä palveluja. Toimija voi olla keskeinen tarjotessaan yhtäkin direktiivin liitteessä mainittua palvelua, mutta tämä ei merkitse, että keskeiseksi toimijaksi tunnistetun organisaation kaikki palvelut olisivat keskeisiä. Direktiivin johdantotekstin kappaleessa 22 mainitaan esimerkkinä, että lentokentän kiitoratapalvelu on kriittinen, mutta lentoaseman myymälätoiminta taas ei ole yhteiskunnan kriittinen palvelu.

Hallituksen esityksen mukaan merkittävää haitallista vaikutusta arvioitaessa tulee huomioida direktiivissä määritellyt seikat kuten palvelusta riippuvaisten käyttäjien lukumäärä, toimijan markkinaosuus sekä toimialakohtaisia kriteereitä. Rautatieliikenteen ja merisatamien osalta konkreettisena esimerkkinä mainitaan osuudet kansallisesta liikennemäärästä ja matkustajien tai rahtikuljetusten lukumäärä vuodessa. (HE 192/2017 vp, s. 38)

NIS-direktiivin 6 artiklassa on merkittävän haitallisen arvioinnin kriteerit. Artikla on systematiikalta jaettu kahteen kokonaisuuteen: Toimialojen väliset kriteerit ja toimialojen sisäiset kriteerit. Toimialojen välisistä kriteereistä jäsenvaltioiden on 6(1) artiklan mukaan otettava huomioon vähintään seuraavat tekijät:

a) toimijan tarjoamasta palvelusta riippuvaisten käyttäjien lukumäärä;
b) muiden toimialojen riippuvuus kyseisen toimijan tarjoamasta palvelusta;

c) poikkeamien vaikutus talouden ja yhteiskunnan toimintoihin tai yleiseen turvallisuuteen[1];

d) kyseisen toimijan markkinaosuus;

e) poikkeaman vaikutuksen maantieteellinen vaikuttavuus;

f) palvelun riittävän tason ylläpitäminen huomioiden vaihtoehtoisten keinojen saatavuus.

NIS-yhteistyöryhmä on laatinut ei-sitovan ohjeistuksen edellä esitettyjen toimialojen välisten kriteerien tulkinnasta. (NIS CG, 2018b, ss. 18-23) Yhteistyöryhmän ohjeistusta käsitellään tarkemmin, kun myöhemmin tutkielmassa havaitaan, että edellä mainitut kriteerit muodostuvat oleellisiksi myös tietoturvahäiriön merkittävyyttä arvioitaessa.

NIS-direktiivin 6(2) artiklan mukaan jäsenvaltioiden on tarvittaessa huomioitava toimialakohtaiset kriteerit. Toimialakohtaisten kriteerien huomioimista vaikeuttaa, että niitä ei ole artiklassa määritelty. Artiklan sanamuodon perusteella on tehtävissä vain johtopäätös, että toimialakohtaiset kriteerit ovat jotakin muuta, kuin toimialojen väliset kriteerit. Toimialan sisäisten kriteerit huomioimiseksi tulkinta-apua saa direktiivin johdannosta. Direktiivin johdantotekstin kappaleiden 26-28 mukaan toimialakohtaisia kriteerejä voisivat olla:

a) palveluntarjoajien lukumäärä,
b) palveluntarjoajan koko esimerkiksi markkinaosuuden tai tuotettujen taikka välitettyjen määrien suhteen,
c) käyttäjien lukumäärä käsittäen sekä henkilökohtaiset käyttäjät että ammatillisesti palvelusta riippuvaiset käyttäjät,
d) onko palvelun käyttö suoraa, epäsuoraa vai välillistä ja
e) liikenteen osalta lento- ja rautatieliikenteen sekä merisatamien osalta osuus kansallisesta liikennemäärästä ja matkustajien tai rahtikuljetusten lukumäärä vuodessa.

Toimialojen välisille sekä toimialakohtaisille kriteereille yhteistä on, että niillä ei ole tärkeysjärjestystä tai ennalta annettua painoarvoa suhteessa toisiinsa. Myöskään yksikään kriteeri ei muodosta niin sanottua ehdotonta edellytystä. Ehdottomalla edellytyksellä tarkoitetaan, että kriteerin täyttäminen tai täyttämättä jättäminen ratkaisi arvioinnin lopputuloksen. Toimialojen väliset kriteerit ovat direktiivin sanamuodon mukaisesti otettava huomioon, kun taas toimialakohtaiset kriteerit ohjeistavat eivätkä sido jäsenvaltioita. Vaikka direktiivin sanamuodon mukaan jäsenvaltioiden on otettava huomioon toimialojen väliset kriteerit, niiden sanamuodosta ei ole pääteltävissä mitään tiettyä tasoa, jonka ylittyessä jäsenvaltioiden olisi määritettävä tietty keskeisen palvelun tarjoaja kansallisen

[1] Direktiivin johdantokappaleen 26 lisäys: "Arvioidessaan vaikutusta, joka poikkeamalla voisi vakavuutensa ja kestonsa perusteella olla talouden ja yhteiskunnan toimintoihin tai yleiseen turvallisuuteen, jäsenvaltioiden olisi arvioitava myös aika, joka todennäköisesti kuluu, ennen kuin palvelun keskeytymisellä alkaisi olla kielteinen vaikutus."

sääntelyn soveltamisalaan kuuluvaksi ja siten velvolliseksi huolehtimaan tietoturvallisuudesta.

Direktiivin jättäessä jäsenvaltioille huomattavaa liikkumavaraa olisi kansallisesti mahdollista pohtia muita, mahdollisesti selkeämpien kriteerien käyttöä keskeisten palveluiden tarjoajien määrittämiseen. Hallituksen esityksessä viitataan LVM:n NIS-direktiivin kansallista täytäntöönpanoa tukevan työryhmän loppuraporttiin, jossa ehdotettiin yksinkertaisempaa soveltamisalaratkaisua. Ehdotetun ratkaisun mukaan arvioidaan mitä palveluita kansallisesti pidetään direktiivin tarkoittamina keskeisinä palveluina. Mikäli nykyisestä lainsäädännöstä ei löydy direktiiviä vastaavaa velvollisuutta tietoturvasta huolehtimisille, niin näiden toimijoiden osalta velvoitteet säädettäisiin osana verkko- ja tietojärjestelmien turvallisuusdirektiivin täytäntöönpanoa. (HE 192/2017 vp, s. 45) Muita vaihtoehtoja voisi olla esimerkiksi tukeutua yhteiskunnan turvallisuusstrategiassa tunnistettuihin toimintoihin tai esimerkiksi harkita, minkälaista hyötyä kilpailuoikeudessa kehitetyistä markkina-aseman merkittävyyden arviointikriteereistä voisi olla ja olisiko niiden kriteerien soveltaminen tietyillä toimialoilla tarkoituksenmukaista. Pohdinnan arvoista voisi olla, olisiko mahdollista kansallisesti määrittää luonnollisen monopolin muodostavien tai määräävässä markkina-asemassa olevien toimijoiden palveluiden tarjonnan keskeytyessä, että kyseessä olisi aina merkittävä haitallinen vaikutus yhteiskunnalle.

Johtopäätöksenä todetaan, että NIS-direktiivistä on johdettavissa arviointikriteerejä keskeisten palveluiden tarjoajien määrittämiseksi. Arviointikriteerit eivät kuitenkaan ole sisällöltään yksiselitteisiä, mikä mahdollistaa jäsenvaltioille merkittävän harkintavallan ja liikkumavaran keskeisten toimijoiden määrittämiseksi. Toisin sanoen viime kädessä kysymys on jäsenvaltioiden lainsäädännössä tai viranomaispäätöksissä tehtävästä kokonaisharkinnasta. Kuitenkin sellaisessa tapauksessa, missä 6(1) artiklan toimialojen välisiä arviointikriteerejä ei ole hyödynnetty, on mahdollista oikeudellisesti perustella, että jäsenvaltio ei olisi toteuttanut direktiivin vähimmäisvaatimusta. Direktiivin arviointikriteeristö tarjoaa jäsenvaltioille mahdollisuuden luoda lainsäädäntöön selkeät ja ennakoitavat kriteerit, joiden perusteella kasvavat ja kriittisemmiksi muodostuvat yhtiöt sekä esimerkiksi julkisiin hankintoihin osallistuvat yhtiöt voisivat paremmin ennakoida, milloin verkko- ja tietojärjestelmien turvallisuussääntely mahdollisesti tulee koskemaan yhtiön toimintoja. Lopuksi on vielä syytä korostaa, että vaikka organisaatio luokiteltaisiin yhteiskunnan keskeisen palvelun tarjoajaksi, tämä ei automaattisesti merkitse sitä, että organisaation kaikki palvelut kuuluisivat sääntelyn soveltamisalaan.

2.1.1 Raideliikenteen keskeisten palveluiden tarjoajien määrittely

Raideliikenteen keskeisten toimijoiden määrittely Suomessa on toteutettu raideliikennelaissa. Voimassa olevan raideliikennelain 169 §:n 1 momentin mukaan valtion rataverkon haltijan sekä liikenneohjauspalvelun tarjoajan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. Pykälä vastaa aikaisempaa NIS-direktiivin kansallisen täytäntöönpanon yhteydessä säädettyä rautatielain 41 a §:ää, eikä sen sisältöön esitetty

muutoksia uutta raideliikennelakia säädettäessä. (HE 105/2018 vp, s. 127) Liikenne- ja viestintäviraston mukaan tällä hetkellä pykälää sovelletaan Väylävirastoon valtion rataverkon haltijana ja Fintraffic Raide Oy:öön liikenteenohjauspalveluiden tarjoajana. (Traficom, 2022) Sen sijaan yksityisraiteiden sekä kaupunkiraideliikenteen haltijat ja rautatieliikenteen harjoittajat kuten VR-Yhtymä Oy on jätetty soveltamisalan ulkopuolelle. Tässä kappaleessa käydään lyhyesti läpi, mistä syistä liikenteenohjauspalvelut sekä valtion rataverkko on sisällytetty verkko- ja tietojärjestelmien turvallisuusvaatimusten piiriin sekä erityisesti pohditaan syitä, miksi yksityisraiteet ja raideliikenteen harjoittajat on jätetty soveltamisalan ulkopuolelle.

Hallituksen esityksen kirjoittamisajankohtana Fintraffic Raide Oy:n tuottamien liikenteenohjauspalveluiden sisällyttäminen keskeiseksi palveluksi oli hallituksen esityksen mukaan useista syistä perusteltua: Liikenteenohjaus on liikennejärjestelmän toimivuuden kannalta keskeistä, vaikuttaa välittömästi liikennejärjestelmän turvallisuuteen, häiriöt voivat johtaa liikenneturvallisuuden vaarantumiseen taikka liikenteen keskeytymiseen, liikenneohjauspalvelut ovat keskitetysti riippuvaista pienestä joukosta toimijoita sekä älykkään automaation yleistyessä liikenteenohjauspalveluiden merkitys korostuu. (HE 192/2017 vp, ss. 46-47) Valtion rataverkko tunnistettiin keskeiseksi palveluksi, koska vuonna 2016 rautateillä kulki 82 miljoonaa henkilömatkustajaa, tavarakuljetusten määrä oli vuonna 2014 noin 37 miljoonaa tonnia ja kuljetussuorite oli noin 9,6 miljardia tonnikilometriä.

Osana Väylävirastolle tuotettavaa liikenteenohjauspalveluiden kokonaisuutta Fintraffic Raide Oy vastaa valtion rataverkolla ratapihojen liikenteenohjauksesta. Voimassa olevassa lainsäädännössä tai hallituksen esityksessä ei kuitenkaan suoraan oteta kantaa ulkoistustilanteisiin. Fintraffic on ulkoistanut osan ratapihojen liikenteenohjauksesta ja kilpailuttanut ulkoistuksen julkisena hankintana. (HILMA, 2020) Kilpailutuksen voittivat VR-Yhtymä Oy ja Destia Rail Oy. (Fintraffic, 2021) Raideliikennelain 169 §:n sanamuodon mukaan verkko- ja tietojärjestelmien turvallisuusvelvoitteet koskevat liikenteenohjauspalvelun tarjoajaa. Pykälän sanamuodonmukainen tulkinta puoltaisi tulkintavaihtoehtoa, että ratapihojen liikenteenohjauksen tarjoaviin yhtiöihin sovellettaisiin verkkoja tietojärjestelmien turvallisuusvelvoitteita. Tämä olisi myös looginen tulkintavaihtoehto, koska pykälän velvoitteita sovelletaan liikenteenohjauspalvelun tarjoajaan eli soveltaminen kattaa lähtökohtaisesti kaiken liikenteenohjauspalveluntarjoamisen valtion rataverkolla. Liikenteenohjauspalvelun tarjoajan ulkoistaessa verkko- ja tietojärjestelmien turvallisuussääntelyn soveltamisalaan kuuluvan osa-alueen liikenteenohjauksesta, ulkoistuksen ei tulisi kaventaa velvoitteiden soveltamisalaa. Toisaalta sanamuodon mukainen tulkinta ei välttämättä olisi säädöksen tarkoituksen mukainen, koska verkko- ja tietojärjestelmien turvallisuussääntelyn ulottamista kilpailutilanteessa toimiviin liikenteenharjoittajiin vältteltiin hallituksen esityksessä. Lisäksi useassa kohdassa hallituksen esitystä mainitaan yksikössä vain yksi yhtiö. Toisaalta yksikkösanamuodon käyttäminen enemmänkin viittaa siihen, että lakia säädettäessä ei ennakoitu useamman liikenteenohjauspalvelun tarjoamisen olevan vaihtoehto. (HE 192/2017 vp, ss. 1, 52, 53,

59, 69) Luonnollisesti myös lainsäädännön soveltamisratkaisuun käytännössä vaikuttaa, onko kyseisten kilpailutukseen kuuluneiden ratapihojen liikenteenohjaus tosiasiallisesti riippuvainen viestintäverkoista tai tietojärjestelmistä.

Nykymuodossa metro- ja raitioliikenteen liikenteenohjaukseen ei sovelleta 169 §:n verkko- ja tietojärjestelmien turvallisuusvelvoitteita, mutta soveltaminen voisi mahdollisesti ajankohtaistua, mikäli kaupunkirataverkon hallinta ja liikenteenohjauspalveluiden tuottaminen eriytettäisiin tulevaisuudessa. Raideliikennelain soveltamisalaa koskevan 3.5 §:n mukaisesti kaupunkiraideliikenteen rataverkon haltijaa ei koske raideliikennelain 169 §, jonka mukaan liikenteenohjauspalvelun tarjoajan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. Raideliikennelain 159 §:n mukaan metro- ja raitioverkon liikenteenohjauksen järjestämisestä vastaa rataverkon haltija, kaupunkiraideliikennettä harjoittava kunnallinen liikelaitos, yhtiö tai muu yhteisö toiminnanharjoittajana. Pääkaupunkiseudulla metro- ja raitioliikenteen liikenteenohjauspalveluista on aikaisemmin vastannut HKL:n liikennöintiyksikkö ja HKL:n omaisuudenhallintayksikkö vastasi joukkoliikenneinfrastruktuurin omaisuuden hallinnasta. HKL on kunnallinen liikelaitos ja osa Helsingin kaupunkia. (Helsinki, 2021) Kun HKL oli sekä rataverkon haltija että liikenteenohjauspalvelun tarjoaja, HKL:n liikenteenohjaukseen ei sovellettu 169 §:n verkko- ja tietojärjestelmien turvallisuusvelvoitteita. HKL muuttui 1.2.2022 Helsingin ja Vantaan kaupunkien omistamaksi Kaupunkiliikenne Oy:ksi, joka nykyisin vastaa muun muassa metro- ja raitiovaunuliikenteestä. (Kaupunkiliikenne, 2022) Kaupunkiliikenne Oy:n vastatessa HKL:n tavoin sekä kaupunkirataverkon hallinnasta sekä liikenteenohjauksesta, verkko- ja tietojärjestelmien turvallisuusvelvoitteita ei edelleenkään sovelleta pääkaupunkiseudun kaupunkiraideliikenteeseen.

Raideliikennelain 3, 159 ja 169 §:ien sanamuotoa yhdessä luettaessa vaikuttaisi siltä, että mikäli kaupunkiraideliikenteessä metro- tai raitioverkon liikenteenohjauksen järjestämisestä vastaisi jokin muu taho kuin kaupunkiraideliikenteen rataverkon haltija, tällöin 169 §:n velvoitteita voitaisiin kaupunkiraideliikenteen liikenteenohjaukseen soveltaa. Toisaalta tällaista nykyistä soveltamiskäytäntöä laajentavaa tulkintaa vastaan on myös mahdollista argumentoida. NIS-direktiivin täytäntöönpanoa koskevassa hallituksen esityksessä liikenteenohjauksella pyrittiin tarkoittamaan valtion rataverkon liikenteenohjausta ja 169 §:n sanamuotoa olisi mahdollista tulkita suppeasti niin, että se koskisi vain valtion rataverkon liikenteenohjauspalveluita.

Raideliikennepalveluiden tarjoamista eli käytännön kuljetustoimintaa raiteilla ei hallituksen esityksen mukaan pidetä yhteiskunnan keskeisenä palveluna. Hallituksen esityksessä linjausta on perusteltu sillä, että liikennepalveluita tarjotaan kilpailutilanteessa, palveluja voidaan järjestää vaihtoehtoisella tavalla vaihtoehtoisen kuljetusmuodon tai kansainvälisen kilpailun ansiosta, liikennepalveluiden luonne muuttuu kansainväliseen suuntaan ja "tietoturvallisuutta voidaan tulevaisuudessa kehittää kohdennetummin ja harmonisoidummin osana kulkumuotokohtaisten kansainvälisten sopimusvelvoitteiden ja EU-säädösten valmistelua", jolla voidaan välttää liikennejärjestelmän toimintaan, turvallisuuteen ja

kansainvälisiin kilpailuedellytyksiin liittyvät häiriöt. Hallituksen esityksessä toisaalta myös todettiin, että osa kotimaisten palveluiden tarjoamisesta on keskittynyt harvoille tai vain yhdelle toimijalle. (HE 192/2017 vp, s . 49)

Suomen kansallisen lainsäädännön näkökulmasta on edellä esitetyn mukaisesti selvää, että rautatieliikenteenharjoittajiin verkko- ja tietojärjestelmien turvallisuusvelvoitteita ei rautatieliikennettä harjoitettaessa sovelleta, koska heitä ei ole raideliikennelain 169 §:ssä mainittu. Seuraavaksi tarkastelen raideliikenteenharjoittajia NIS-direktiivin näkökulmasta ja arvioin, olisiko raideliikenteenharjoittajat tullut direktiivin mukaan sisällyttää osaksi kansallista lainsäädäntöä. Arvioinnin toteutan kappaleessa 2.1. Liikennejärjestelmän keskeiset palvelut esittelemäni kolmekohtaisen arviointikriteeristön kautta eli arvioimalla a) tarjoaako toimija palvelua, joka on keskeinen yhteiskunnan ja/tai talouden kriittisten toimintojen ylläpitämiseksi, b) onko kyseisen palvelun tarjoaminen riippuvainen verkko- ja tietojärjestelmistä ja c) olisiko poikkeamalla merkittäviä haitallisia vaikutuksia kyseisen palvelun tarjoamiseen.

Ensimmäiseen arviointikohtaan (a) vastaaminen on suhteellisen suoraviivaista, koska rautatieyritykset rautatieliikenteen harjoittajina mainitaan direktiivin liitteen listassa. NIS-direktiivin liitteen mukaan raideliikenteen keskeisiä toimijoita ovat rataverkon haltijat ja rautatieyritykset, mukaan lukien palvelupaikan ylläpitäjät. Raideliikenteen keskeisten toimijoiden tarkempi määrittely perustuu NIS-direktiivin liitteen viittauksella Euroopan parlamentin ja neuvoston direktiivin 2012/34/EU (myöh. rautatiemarkkinadirektiivi) määritelmiin.

Rautatieyrityksellä rautatiemarkkinadirektiivin 3(1) artiklan mukaan tarkoitetaan rautatiemarkkinadirektiivin mukaisesti toimiluvan saanutta julkista tai yksityistä yritystä, jonka päätoimena on rautateiden tavara- ja/tai henkilöliikenteen harjoittaminen ja joka on velvollinen huolehtimaan vetopalveluista; tähän kuuluvat myös yksinomaan vetopalveluja tarjoavat yritykset.

Palvelupaikan ylläpitäjät luetaan NIS-direktiiviä sovellettaessa rautatieyrityksiksi ja niillä tarkoitetaan rautatiemarkkinadirektiivin 3(12) artiklan mukaan julkista tai yksityistä yhteisöä, joka vastaa yhden tai useamman palvelupaikan hallinnoinnista tai joka tarjoaa rautatieyrityksille yhtä tai useampaa liitteessä II olevissa 2–4 kohdassa tarkoitettua palvelua. Rautatiemarkkinadirektiivin liitteen II kohdat 2-4 muodostavat 17 kohtaisen listan palveluita, joista tärkeimpinä voitaneen pitää matkustaja-asemia, tavaraliikenneterminaaleja, järjestelyratapihoja ja junanmuodostuslaitteita, mukaan lukien vaihtotyölaitteet, varikkosivuraiteita, rautatietoimintaan liittyviä meri- ja sisävesisatamien varusteita, tankkauspalveluja, kuljetussähkövirtaa, vaarallisten aineiden kuljetusten valvonnasta tehtyjä sopimuksia ja perusteellisia huoltopalveluja.

Arviointikohtaan (b) onko kyseisen palvelun tarjoaminen riippuvainen verkko- ja tietojärjestelmistä vastaan oletuksella, että nykyisten kaltaisten rautateiden matkustajamäärä ja tavararahtia ei olisi yhtä sujuvasti mahdollista hallinnoida ilman tietotekniikkaa. Arviointikohtaan täsmällisempi vastaaminen edellyttäisi tarkempaa tietoa esimerkiksi VR-Yhtymä Oy:n sisäisistä tietojärjestelmistä ja prosesseista, joita käytetään liikennettä harjoitettaessa. Yksittäisen yhtiön järjestelmien selvittäminen ei kuitenkaan tämän tutkimuksen puitteissa ole

tarkoituksenmukaista ja siten tyydyn olettamaan, että raideliikenteenharjoittaminen on tavalla tai toisella riippuvaista verkko- ja tietojärjestelmistä.

Arviointikohdan (c) olisiko poikkeamalla merkittäviä haitallisia vaikutuksia kyseisen palvelun tarjoamiseen tulee kappaleessa 2.1. esitetyllä tavalla arvioida toimialojen välisten sekä toimialojen sisäisten kriteerien perusteella, joista direktiivin sanamuodon mukaan jäsenvaltioiden on otettava huomioon vähintään direktiivin 6(1) artiklassa mainitut toimialojen väliset tekijät. Hallituksen esityksessä näiden tekijöiden arviointi on puutteellista, koska hallituksen esityksessä kuuden kohdan listasta arviointi toteutui vain yhden kohdan eli vaihtoehtoisten keinojen saatavuuden osalta. Vaihtoehtoisista keinoista hallituksen esityksessä todettiin, että voi olla keinoja järjestää palvelu vaihtoehtoisella tavalla kansainvälisen kilpailun tai vaihtoehtoisten kuljetusmuotojen ansiosta. Hallituksen esityksessä ei arvioitu toimijan palveluista riippuvaisten käyttäjien määrää[2] [3], muiden toimialojen riippuvuutta toimijan palvelusta[4], poikkeaman vaikutuksia talouden tai yhteiskunnan toimintoihin[5], toimijan markkinaosuutta[6] taikka maantieteellistä kattavuutta. Edellä esitetyn perusteella on mahdollista tehdä johtopäätös, että hallituksen esityksessä on puutteellisesti perusteltu ja määritetty keskeisten palveluiden tarjoajat rautatieyritysten osalta. Toisaalta vaikka hallituksen esityksessä ei ole toteutettu NIS-direktiivin 6 artiklan mukaista merkittävän haitallisen vaikutuksen arviointia, niin kappaleessa 2.1. esitetyn mukaisesti 6 artiklan kriteereillä ei ole tärkeysjärjestystä, eikä mikään muodosta niistä ehdotonta edellytystä lopputulokselle. Toisin sanoen merkittävän haitallisen vaikutuksen arvioinnin jälkeen olisi silti voinut olla mahdollista tehdä poliittinen päätös rautatieyritysten jättämisestä direktiivin soveltamisalan ulkopuolelle, koska direktiivin artiklojen väljä sanamuoto tämän mahdollistaa.

NIS-direktiivin näkökulmasta tavaraliikenneterminaaleja hallinnoivia palvelupaikan ylläpitäjiä pidetään rautatieyrityksinä ja siten jäsenvaltiot voisivat soveltaa tavaraliikenneterminaaleihin verkko- ja tietojärjestelmien turvallisuussääntelyn velvoitteita. Vesiliikenteessä yhteiskunnan keskeisinä palveluina pidettävät satamat on määritetty viittaamalla Euroopan parlamentin ja neuvoston asetukseen 1315/2013 unionin suuntaviivoista Euroopan laajuisen liikenneverkon kehittämiseksi ja päätöksen 661/2010/EU kumoamisesta (TEN-T asetus).

---

[2] Rautateiden henkilöliikenteessä vuonna 2019 tehtiin lähes 15 000 kaukoliikenteen ja lähes 78 000 lähiliikenteen matkaa. (Väylävirasto, 2021)

[3] Valtio ostaa VR-Yhtymä Oy:ltä velvoitejunaliikennettä yli 20 miljoonan euron arvosta. (LVM, 2019)

[4] Henkilöliikenteessä VR-Yhtymä Oy on ainoa palveluntarjoaja. Raideliikenteen osuus kotimaan tavaraliikenteen on noin 25%. (Liikennevirasto, 2018, s. 27)

[5] Yhteiskunnan turvallisuusstrategian mukaan väestön toimeentulolle ja elinkeinoelämälle kriittiset kuljetukset ovat yksi keskeinen palvelu ja tämän takia varautumisvelvoite on sisällytetty muun muassa rautatieliikenteen harjoittajille ja metroliikenteen harjoittajalle. (Turvallisuuskomitea, 2017, s. 66)

[6] Henkilöliikenteen markkinaosuus on noin viisi prosenttia henkilöliikenteestä. (Liikennevirasto, 2018, s. 26)

TEN-T asetuksen liitteessä Suomen ainoaksi ydinverkon rautatie- ja maatieterminaaliksi on määritetty Kouvola. Kouvolan kaupungin mukaan terminaali on tarkoitus ottaa käyttöön 2023 ja siellä on tarkoitus pystyä käsittelemään yli kilometrin pituisia junia kokonaisina. (Kouvola, 2021) Hallituksen esityksessä ei ole ollut mahdollisuuksia arvioida Kouvolan terminaalin merkitystä raideliikenteen verkko- ja tietojärjestelmien turvallisuuden näkökulmasta. Kuitenkin hallituksen esityksessä luotu kategorinen ratkaisu raideliikenneyritysten, raideliikenteen harjoittajien ja yksityisraiteiden omistajien sulkemiseksi soveltamisalueen ulkopuolelle ei Kouvolan TEN-T ydinverkon terminaalin osalta ole johdonmukaisesti perusteltu, koska samalla TEN-T verkon merkityksellä satamien merkittävyys pystytään perustelemaan, kuten jäljempänä satamia koskevassa kappaleessa todetaan.

Kaupunkiraideliikenteen rataverkon haltijoita ja yksityisraiteiden omistajia ei Suomessa ole sisällytetty NIS-sääntelyn soveltamisalaan. NIS-direktiivissä rataverkon haltijat on sisällytetty direktiivin soveltamisalaan viittauksella rautatiemarkkinadirektiiviin. *Rataverkon haltijalla* rautatiemarkkinadirektiivin 3(2) artiklan mukaan tarkoitetaan elintä tai yritystä, joka on vastuussa erityisesti rautatieinfrastruktuurin rakentamisesta, hallinnoinnista ja kunnossapidosta, mukaan lukien liikenteen hallinta sekä ohjaus, hallinta ja merkinanto; verkkoa tai verkon osaa koskevat rataverkon haltijan tehtävät voidaan antaa eri elimille tai yrityksille. Direktiivin määritelmä rataverkon haltijoista mahdollistaisi arvioinnin, tulisiko esimerkiksi Tampereen Raitiotie Oy tai pääkaupunkiseudun Kaupunkiliikenne Oy kaupunkiraideliikenteen rataverkon haltijana sisällyttämisen verkko- ja tietojärjestelmien turvallisuussääntelyn piiriin. Tällöinkään sääntely ei direktiivin mukaan koskisi kaupunkiraideliikenteen harjoittamista. On kuitenkin syytä muistaa, että NIS-direktiivi on minimiharmonisoiva direktiivi eli Suomi voisi halutessaan ylittää direktiivin vaatimukset ja ulottaa sääntelyn myös kaupunkiraideliikenteenharjoittamiseen. Lisäksi sanamuodon mukainen tulkinta mahdollistaisi myös yksityisraiteiden haltijoiden sisällyttämisen sääntelyn piiriin. Yksityisraiteella tarkoitetaan muuta kuin valtion omistamaa ja valtion rataverkon hallinnoimaa raideliikennelain mukaista raidetta (Raideliikennelaki 4 § kohta 56). Suomessa on 126 yksityisraiteen haltijaa. (Traficom, 2021a) Selkeyden vuoksi on syytä todeta, että rautatiemarkkinadirektiivi sisältää pakottavia soveltamisalan rajauksia sekä jättää jäsenvaltioille harkintavaltaa, miltä osin direktiiviä sovelletaan esimerkiksi kaupunkiraideliikenteen harjoittajaan (art. 2.1), alueellisiin rautatieliikenneyrityksiin (art. 2.2) ja yksityisraiteiden haltijaan (art. 2.3). Nämä rautatiemarkkinadirektiivin soveltamisalan rajaukset eivät kuitenkaan merkitse, etteikö NIS1-direktiiviä voisi näihin soveltaa.

Hallituksen esityksessä yksityisraiteiden osalta perustelut ja poikkeamien merkittävyyden arviointi ovat lyhyet: "Yksityisraiteet voivat sinänsä olla esimerkiksi tietyn teollisuuslaitoksen tai esimerkiksi sataman kannalta merkityksellisiä. Niiden ylläpitäminen ei kuitenkaan ole samalla tavalla yhteiskunnan toiminnan kannalta keskeistä kuin valtion rautateiden." (HE 192/2017 vp, s. 48) Yhdyn hallituksen esityksen näkemykseen yksityisraiteista siltä osin, kun tarkastellaan yksittäisen teollisuuslaitoksen raiteita. Kuitenkin satamien kohdalla mielestäni

Suomen sektorikohtainen NIS-direktiivin täytäntöönpano osoittaa heikkoutensa, koska seuraavassa kappaleessa todetaan satamien ja satamarakenteiden kuuluvan Suomessa verkko- ja tietojärjestelmien turvallisuussääntelyn piiriin, mutta satamissa sijaitsevat tai niihin johtavat yksityisraiteet jäävät kuitenkin soveltamisalan ulkopuolelle. Raideliikenteen merkitys Suomen ulkomaansatamille on suuri ja häiriöt raideliikenteessä voivat heijastua häiriöinä satamien logistiikkatoiminnoissa ja päinvastoin. Esimerkiksi heinäkuussa 2021 Etelä-Afrikan Kapkaupungissa operoivaan Transnet yritykseen kohdistunut kyberhyökkäys lamaannutti usean yrityksen konttiterminaalin lastinkäsittelyn, mikä johti raideliikenteen jumiutumiseen ja kilometrien rekkajonoihin. (Ginindza, 2021)

Yhteenvetona yhteiskunnan keskeisten palveluiden määrittämisestä raideliikennesektorilla voidaan todeta sääntelyn koskevan Väylävirastoa valtion rataverkon haltijana ja Fintraffic Raide Oy:tä raideliikenteen ohjauspalveluiden tarjoajana. Raideliikenteenohjauspalveluiden osittainen ulkoistaminen tiettyjen ratapihojen osalta on luonut lainsäädännön soveltamisen kannalta epäselvän tilanteen. Tilanteen tulkinnanvaraisuudesta huolimatta puoltaisin kantaa, että nykyisestä Traficomin tulkinnasta huolimatta ulkoistuksen seurauksena lainsäädännön velvoitteet koskisivat myös VR Yhtymä Oy:tä sekä Destia Rail Oy:tä siltä osin, kun kyse on ulkoistuksen kohteena olevan liikenteenohjauspalvelun tuottamisesta. Suomen kansallisen lainsäädännön osalta on selvää, että rautatieliikenteenharjoittajia ei pidetä yhteiskunnan kannalta keskeisen palvelun tarjoajana eli heihin velvoitteita ei sovelleta. Kuitenkin katson, että hallituksen esityksessä on puutteellisesti perusteltu ja määritetty keskeisten palveluiden tarjoajat rautatieyritysten osalta. Kouvolaan vuonna 2023 valmistuva Suomen ainoa TEN-T ydinverkon rautatie- ja maaliikenneterminaali ei myöskään nykyisten säädösten mukaan tulisi kuulumaan yhteiskunnan keskeisiin palveluihin, vaikka vastaavan korkeimman luokan satamat yhteiskunnan keskeisiksi palveluiksi luetaankin. NIS-direktiivin viittaukset rautatiemarkkinadirektiivin vaikuttaisivat mahdollistavan myös kaupunkiraiteiden haltijoiden kuten pääkaupunkiseudun Kaupunkiliikenne Oy:n ja Tampereen Raitiotie Oy:n sisällyttämisen rataverkon haltijoina sääntelyn piiriin, mutta tällaista näkökulmaa ei kansallisesti ole arvioitu. Yksityisraiteiden haltijat eivät myöskään kuulu yhteiskunnan keskeisiin palveluihin, mutta erityisesti satamaraiteiden osalta niillä on erittäin tärkeä rooli yhteiskunnan logistiikkaketjuissa ja niiden sisällyttämistä sääntelyn piiriin tulisi tulevaisuudessa arvioida uudelleen.

2.1.2 Vesiliikenteen keskeisten palveluiden tarjoajien määrittely

Vesiliikenteessä verkko- ja tietojärjestelmien turvallisuussääntelyä Suomessa sovelletaan meriliikenteen ohjauspalvelua tarjoavaan Fintraffic Meriliikenteenohjaus Oy:öön (VTS-palvelu, Vessel Traffic Service) sekä Turun, Naantalin, Hamina-Kotkan ja Helsingin satamiin. (Kyberturvallisuuskeskus, 2021) Meriliikenteenohjausta koskeva verkko- ja tietojärjestelmien turvallisuussääntely on sisällytetty alusliikennepalvelulain 16.5 ja 18 a §:ään. Satamia koskeva vastaava säädös on sisällytetty lakiin eräiden alusten ja niitä palvelevien satamien turva-

toimistoimista ja niiden valvonnasta (Turvatoimilaki) 7 e ja 7 f §:iin. Suomen suurinta tavaraliikennesatamaa sekä varustamoita ei verkko- ja tietojärjestelmien turvallisuusvelvoitteiden näkökulmasta pidetä yhteiskunnan keskeisinä palveluina. Kuitenkin NIS-direktiivin liitteen näkökulmasta vesiliikenteen keskeisiä toimijoita voivat olla matkustaja- ja rahtiliikennettä hoitavat yhtiöt lukuun ottamatta yksittäisiä aluksia, satamien hallintoelimet satamarakenteet mukaan lukien sekä satamien alueella tuotantolaitoksista ja laitteista huolehtivat toimijat. Direktiivitasolla vesiliikenteen keskeisten palveluiden määrittely on toteutettu liitteessä viittaamalla Euroopan parlamentin ja neuvoston asetukseen 725/2004 alusten ja satamarakenteiden turvatoimien parantamisesta (myöh. turvatoimiasetus), Euroopan parlamentin ja neuvoston direktiivi 2005/65/EY satamien turvallisuuden parantamisesta (myöh. satamaturvadirektiivi) ja Euroopan parlamentin ja neuvoston direktiivi 2002/59/EY alusliikennettä koskevan yhteisön seuranta- ja tietojärjestelmät perustamisesta (myöh. valvontadirektiivi).

Alusliikennepalvelut ovat hallituksen esityksen mukaan keskeinen palvelu, koska liikenteenohjaus on liikennejärjestelmän toimivuuden kannalta keskeistä, vaikuttaa välittömästi liikennejärjestelmän turvallisuuteen, häiriöt voivat johtaa liikenneturvallisuuden vaarantumiseen taikka liikenteen keskeytymiseen, liikenneohjauspalvelut ovat keskitetysti riippuvaista pienestä joukosta toimijoita sekä älykkään automaation yleistyessä liikenteenohjauspalveluiden merkitys korostuu. (HE 192/2017 vp, ss. 46-47) Suomessa Väylävirasto vastaa hallinnoimillaan väylillä alusliikennepalvelun järjestämisestä ja niiden käytännön tarjoamisesta vastaa Fintraffic Meriliikenteenohjaus Oy. Suomen merialue on jaettu kuuteen alusliikennepalvelut (VTS) alueeseen sekä Saimaan syväväylän alueeseen. Meriliikenteenohjaukset keskukset sijaitsevat Turussa, Helsingissä ja Lappeenrannassa. (Väylävirasto, päiväämätön) Alusliikennepalveluiden osalta sääntelyn soveltamisala on suhteellisen selkeä ja kuten kappaleen loppupuolella tulen toteamaan, Suomen lainsäädäntö on myös yhdenmukainen tuoreemman EU:n komission täytäntöönpanoasetuksen kanssa koskien sisävesien AIS-järjestelmiä. Raideliikenteestä poiketen Väylävirasto ei ole verkko- ja tietojärjestelmien turvallisuussääntelyn kohteena hallinnoimiensa meri- ja sisävesiväylien osalta. Täten esimerkiksi Väyläviraston ylläpitämät merenkulun turvalaitteet kuten linjamerkit, loistot ja merimajakat eivät kuulu sääntelyn piiriin. Toisaalta useiden merenkulun turvalaitteiden kanssa on samanlainen tilanne kuin tieliikenteessä eli suuri osa turvalaitteista ei ole vielä riippuvaisia verkkoyhteyksistä ja tietojärjestelmistä.

Vesiliikenteen toisen yhteiskunnan keskeisten palveluiden tarjoajien kategorian muodostavat satamien hallintoelimet, joilla satamaturvadirektiivin 3(1) artiklan mukaan tarkoitetaan määrättyä maa- ja vesialuetta, jonka rajat sataman sijaintijäsenvaltio määrittää ja jonka rakenteet ja varusteet on tarkoitettu kaupallisen merikuljetustoiminnan helpottamiseen. Satamarakenteilla tarkoitetaan satamaturvadirektiivin 3(3) artiklan mukaan paikkaa, jossa sataman ja alusten vuorovaikutus tapahtuu. Siihen kuuluvat soveltuvin osin ankkurointialueet, odotuspaikat ja sisääntuloväylät. Hallituksen esityksen mukaan satamat ovat liikenteen keskeistä infrastruktuuria, koska vuonna 2014 ulkomaankaupan kuljetuksista 96

miljoonaa tonnia oli merikuljetuksia, 11 miljoonaa tonnia maakuljetuksia ja ulkomaankaupasta tonnikilometreissä 96 prosenttia kulki merirahtina. Toisin sanoen elinkeinoelämä ja koko yhteiskunta ovat riippuvaisia satamien toiminnasta. (HE 192/2017 vp, s. 48) Hallituksen esityksessä kuitenkin korostetaan, että kaikkia satamia ei tule sisällyttää sääntelyn piiriin, koska satamien koko vaihtelee: Noin 80 prosenttia merikuljetusten kokonaisvolyymista käsitellään kymmenessä suurimmassa satamassa. Tällöin poikkeaman merkitys yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjoamiseen vaihtelee ja velvoitteiden kohdistamista tulisi arvioida NIS-direktiivin 6 artiklan (merkittävä haitallinen vaikutus) näkökulmasta. (HE 192/2017 vp, s. 52) Turvatoimilain 7 e §:n 3 momentin mukaisesti yhteiskunnan toiminnan kannalta merkittävien satamien määrittely delegoitu säädettävän erillisellä valtioneuvoston asetuksella. Valtioneuvoston asetuksen yhteiskunnan toiminnan kannalta merkittävistä lentoasemista ja satamista (361/2018) mukaan yhteiskunnan toiminnan kannalta merkittävät satamat määritetään EU-asetuksessa. Valtioneuvoston asetuksessa viitataan TEN-T asetukseen, jonka liitteessä II määritellyt ydinverkon merisatamat. Ydinverkon merisatamiksi asetuksessa on määritetty Helsinki, Kotka, Hamina, Turku ja Naantali.

Huomionarvoista TEN-T asetuksessa on, että Suomen suurin tavaraliikennesatama Sköldvik eli Porvoon Kilpilahti (Traficom, 2019) ja kolmanneksi suurin matkustajaliikennesatama Maarianhamina (Suomen satamaliitto, 2018) ovat TEN-T asetuksen liitteessä luokiteltu ydinverkkoa matalampaan, kattavan verkon kategoriaan. Siten näitä satamia ei pidetä yhteiskunnan keskeisinä palveluina Suomen verkko- ja tietojärjestelmien turvallisuuden näkökulmasta. NIS-direktiivin täytäntöönpanoa koskevassa hallituksen esityksessä valtioneuvostolle annettiin asetuksenantovaltuus yhteiskunnan toiminnan kannalta merkittävien satamien määrittämiseksi ja todettiin, että NIS-direktiivin 5(2) artiklan mukaiset kriteerit tulee huomioida arvioitaessa, onko toimija yhteiskunnan toiminnan kannalta merkittävä. (HE 192/2017 vp, s. 74 ja LVM, 2018) Valtioneuvoston asetuksen muistiossa Kilpilahden osalta todetaan, että "Kilpilahden satama eroaa luonteeltaan näistä muista satamista siinä, että se palvelee pääasiallisesti Kilpilahden teollisuusaluetta". (LVM, 2018, s. 6) Tutkimusta tehdessä ei ole löytynyt muuta virallisaineistoa siitä, miksi Suomen suurinta tavaraliikennesatamaa ei tulisi pitää yhteiskunnan keskeisenä toimintona, kun tavaraliikennemäärältään pienempiä satamia tällaisina pidetään. Toisesta näkökulmasta tarkasteltuna erityisesti Yhteiskunnan turvallisuusstrategia puoltaisi Kilpilahden ja Ahvenanmaan satamien pitämistä yhteiskunnan keskeisinä palveluina. Yhteiskunnan turvallisuusstrategian mukaan Suomen huoltovarmuuteen ja ulkomaankauppaan liittyvien kuljetusten jatkuvuuden varmistamiseksi Suomen ulkomaankaupan meriliikenneyhteydet ja satamat varmistetaan niin häiriötilanteessa kuin poikkeusoloissa joko lainsäädäntö-, sopimus- tai muulla vahvalla perusteella, minkä lisäksi elinkeinoelämä osallistuu roolinsa mukaisesti varautumistyöhön. (Turvallisuuskomitea, 2017, s. 68)

Edellä esitetyn tiedon perusteella vaikuttaisi siltä, että valtioneuvoston asetuksessa ei ole toteutunut NIS-direktiivin täytäntöönpanoa koskeva hallituksen

esityksen kirjaus keskeisten palvelujen tarjoajien määrittämisestä (5(2) artikla) siltä osin, kun kyse on Suomen suurimmasta tavaraliikennesatamasta, koska direktiivin mukaisia arviointiperusteita ei ole huomioitu. Lainsäädännön selkeyden ja ennustettavuuden näkökulmasta yhteiskunnan keskeisinä palveluina pidettävien satamien määrittely viittaamalla TEN-T verkon ydinsatamiin on toimiva, mutta mahdollisesti tämän rinnalle olisi tullut painokkaammin harkita määrällisiä tai laadullisia kriteereitä, että myös Kilpilahti ja mahdollisesti myös Ahvenanmaan satamien merkittävyys tulisi tarkemmin arvioitua.

Vesiliikenteessä varustamoita ei Suomessa pidetä yhteiskunnan keskeisenä palveluna eli matkustajaliikennettä, tavaraliikennettä tai jäänmurtopalveluja tarjoavat toimijat eivät kuulu verkko- ja tietojärjestelmien turvallisuussääntelyn piiriin. Sääntelyn ulkopuolelle tällöin jää yhtiöitä kuten Tallink Silja Oy, Viking Line Abp, Finnlines Oyj ja Arctia konserni. (Suomen varustamot, 2021) Hallituksen esityksessä varustamoiden jättämistä lain soveltamisalan ulkopuolelle perusteltiin sillä, että liikennepalveluita tarjotaan kilpailutilanteessa, palveluja voidaan järjestää vaihtoehtoisella tavalla vaihtoehtoisen kuljetusmuodon tai kansainvälisen kilpailun ansiosta, liikennepalveluiden luonne muuttuu kansainväliseen suuntaan ja "tietoturvallisuutta voidaan tulevaisuudessa kehittää kohdennetummin ja harmonisoidummin osana kulkumuotokohtaisten kansainvälisten sopimusvelvoitteiden ja EU-säädösten valmistelua", jolla voidaan välttää liikennejärjestelmän toimintaan, turvallisuuteen ja kansainvälisiin kilpailuedellytyksiin liittyvät häiriöt. Hallituksen esityksessä toisaalta myös todettiin, että osa kotimaisten palveluiden tarjoamisesta on keskittynyt harvoille tai vain yhdelle toimijalle. (HE 192/2017 vp, s. 49)

Seuraavaksi tarkastelen varustamoita NIS-direktiivin näkökulmasta ja arvioin, olisiko varustamot tullut direktiivin mukaan sisällyttää osaksi kansallista lainsäädäntöä. Arvioinnin toteutan kappaleessa 2.1. Liikennejärjestelmän keskeiset palvelut esittelemäni kolmekohtaisen arviointikriteeristön kautta eli arvioimalla a) tarjoaako toimija palvelua, joka on keskeinen yhteiskunnan ja/tai talouden kriittisten toimintojen ylläpitämiseksi, b) onko kyseisen palvelun tarjoaminen riippuvainen verkko- ja tietojärjestelmistä ja c) olisiko poikkeamalla merkittäviä haitallisia vaikutuksia kyseisen palvelun tarjoamiseen.

Ensimmäiseen (a) kohtaan vastaus löytyy NIS-direktiivin liitteestä, jonka mukaan keskeisen palvelun tarjoajat voivat olla sisävesillä, merillä ja rannikoilla matkustaja- ja rahtiliikennettä hoitavia yhtiöitä. Yhtiöiden tarkempi määrittäminen on toteutettu viittaukselle EU:n turvatoimiasetuksen liitteeseen I. Turvatoimiasetuksen liite I viittaa edelleen sopimukseen ihmishengen turvallisuudesta merellä (SOLAS-sopimus) lukuun IX, jossa edelleen IX luvun säännön 1 kohdassa 2 yhtiöllä tarkoitetaan laivan omistajaa tai muuta järjestöä tai liikenteen harjoittajan kaltaista henkilöä taikka ilman miehistöä rahdatun aluksen rahtaajaa, jolla on aluksen omistajan asemasta vastuu aluksen toiminnasta ja joka on vastuun hyväksyttyään myöntynyt ottamaan huolehdittavakseen kaikista kansainvälisessä turvallisuusjohtamissäännöstössä määrätyistä tehtävistä ja velvollisuuksista. NIS-direktiivin liitteessä matkustaja- ja rahtiliikenteen yhtiöiden osalta on erityisesti syytä korostaa, että näiden yhtiöiden liikennöimät yksittäiset

alukset on kategorisesti suljettu NIS-direktiivin soveltamisalan ulkopuolelle. Laivoja omistavat yhtiöt eli varustamot täyttävät (a) kohdan määritelmän, koska ne ovat viittausten kautta sisällytetty NIS-direktiivin liitteeseen II.

Arviointikohtaan (b), onko kyseisen palvelun tarjoaminen riippuvainen verkko- ja tietojärjestelmistä, vastaamiseksi on tärkeää muistaa, että varustamoiden kohdalla arviointi ei käsitä yksittäisiä aluksia, vaan ainoastaan muut varustamoiden toimintojen osa-alueet. Tässä kohtaa tutkimusta tehdään olettama, että Suomen varustamoiden toiminta on suurelta osin digitalisoitunut ja siten riippuvainen verkko- ja tietojärjestelmistä.

Arviointikohdan (c) olisiko poikkeamalla merkittäviä haitallisia vaikutuksia kyseisen palvelun tarjoamiseen tulee kappaleessa 2.1. esittämälläni tavalla arvioida toimialojen välisten sekä toimialojen sisäisten kriteerien perusteella, joista direktiivin sanamuodon mukaan jäsenvaltioiden on otettava huomioon vähintään NIS-direktiivin 6(1) artiklassa mainitut toimialojen väliset tekijät. Hallituksen esityksessä näiden tekijöiden arviointi on puutteellista, koska hallituksen esityksessä kuuden kohdan listasta arviointi toteutui vain vaihtoehtoisten keinojen saatavuuden osalta. Vaihtoehtoisista keinoista hallituksen esityksessä todettiin, että voi olla keinoja järjestää palvelu vaihtoehtoisella tavalla kansainvälisen kilpailun tai vaihtoehtoisten kuljetusmuotojen ansiosta.

Toisaalta jopa vaihtoehtoisten kuljetusmuotojen saatavuus on tämän päivän näkökulmasta kyseenalaista. Koronapandemian aikana huoltovarmuuden, teollisuuden tarpeiden ja liikenneyhteyksien kannalta Liikenne- ja viestintävirasto Traficom piti välttämättömänä palveluvelvoitteen asettamista Turku-Tukholma, Ahvenanmaa-Ruotsi, Helsinki-Tallinna ja Vaasa-Uumaja väleillä, joita pidetään keskisinä merireitteinä. (Traficom, 2021b) Meriliikenteen palveluvelvoitteen oikeusperusta on Valtioneuvoston asetuksessa 548/2020 meriliikenteen tukemisesta, jonka 6 §:n mukaan meriliikenteen julkista palveluvelvoitetta käytetään, jos se on välttämätöntä riittävien liikenneyhteyksien, huoltovarmuuden ja Suomen ulkomaankaupan kuljetusten kannalta. Soveltaminen edellytti myös Huoltovarmuuskeskuksen lausuntoa palveluvelvoitteen välttämättömyydestä huoltovarmuuden kannalta. Tämän päivän näkökulmasta tarkasteltuna NIS-direktiivin täytäntöönpanoa koskevan hallituksen esityksen kirjaus vaihtoehtoisten keinojen saatavuudesta vaikuttaa olleen turhan optimistinen ja tietyillä reiteillä operoivia varustamoita voisi Traficomin päätöksen ja Huoltovarmuuskeskuksen lausunto huomioiden pitää yhteiskunnan kannalta keskeisten palveluiden tarjoamisena. On myös huomioitava, että hallituksen esityksen laatimisen aikaan tieto varustamoiden merkityksestä yhteiskunnan keskeisenä palveluna oli käytettävissä. Yhteiskunnan turvallisuusstrategian mukaan Liikenne- ja viestintäministeriö, Puolustusministeriö ja Työ- ja elinkeinoministeriö vastaavat Suomen huoltovarmuuteen ja ulkomaankauppaan liittyvien kuljetusten jatkuvuuden varmistamisesta. Tarkoituksena on, että "[K]uljetuslogistisen järjestelmän toimivuus ja turvallisuus sekä yhteiskunnan toiminnan ja huoltovarmuuden edellyttämät kriittiset sisäiset ja ulkomaankaupan kuljetukset tarvittavine tukipalveluineen varmistetaan häiriötilanteissa ja poikkeusoloissa". Esimerkiksi Suomen ulkomaankaupan meriliikenneyhteydet, terminaalit ja satamat tunnistetaan

keskeisiksi. Toimintamallina on, että "[K]riittiset yritykset ja palveluntuottajat varmistavat toiminnan jatkuvuuden joko lainsäädäntö-, sopimus- tai muulla vahvalla perusteella". (Turvallisuuskomitea, 2017, s. 68) Huomioiden, että yhteiskunnan turvallisuusstrategian laatiminen ja NIS-direktiivin kansallinen voimaansaattaminen ajoittuvat samaan ajankohtaan ja hallituskauteen, tästä huolimatta NIS-direktiivi saatettiin vesiliikenteessä kansallisesti voimaan selkeästi YTS:n tunnistamaa tavoitetta suppeammin, jolloin muutamia merkittäviä satamia ja terminaaleja sekä varustamot jätettiin tietoturvallisuuden riskienhallintavelvoitteen ulkopuolelle.

Edelleen poikkeaman haitallisen vaikutuksen merkittävyyttä arvioitaessa on syytä huomata, että verkko- ja tieturvadirektiivin täytäntöönpanoa koskevassa hallituksen esityksessä ei arvioitu toimijan palveluista riippuvaisten käyttäjien määrää, muiden toimialojen riippuvuutta toimijan palvelusta, poikkeaman vaikutuksia talouden tai yhteiskunnan toimintoihin, toimijan markkinaosuutta taikka maantieteellistä kattavuutta. Edellä esitetyn perusteella on mahdollista tehdä johtopäätös, että hallituksen esityksessä on puutteellisesti perusteltu, kuinka varustamoihin kohdistuvan tietoturvapoikkeaman merkittävyys on direktiivissä asetettujen kriteerien mukaisesti arvioitu. Edellä esitetyn perusteella 2020-luvun poikkeusolot ja erityisesti niihin liittyvä meriliikenteen palveluvelvoitteen säätäminen sekä soveltaminen osoittaa, että meriliikenteenharjoittajien ja erityisesti varustamoiden jättäminen yhteiskunnan keskeisten palveluiden ulkopuolelle vaatisi uudelleentarkastelua.

NIS-direktiivin hyväksymisen jälkeen vesiliikenteen keskeisten toimijoiden määrittelyä on EU:ssa tarkennettu kahdessa EU:n komission täytäntöönpanoasetuksessa. Ensimmäinen täydennys koskee sisävesien elektronisia merikarttajärjestelmiä (ECDIS-järjestelmä). Komission täytäntöönpanoasetuksen mukaan sisävesien elektroniseen merikarttajärjestelmään sovelletaan NIS-direktiiviä, kun järjestelmä huolehtii keskeisestä[7] palvelusta. (Komission täytäntöönpanoasetus (EU) 2018/1973, Euroopan parlamentin ja neuvoston direktiivissä 2005/44/EY tarkoitetuista sisävesiliikenteen elektronista merikarttajärjestelmää (sisävesien ECDIS-järjestelmä) koskevista teknisistä eritelmistä annetun täytäntöönpanoasetuksen (EU) N:o 909/2013 muuttamisesta, liite 1 jakso 1 art. J kohta) Komission täytäntöönpanoasetus on annettu Euroopan parlamentin ja neuvoston yhdenmukaisista jokitiedotuspalveluista (RIS) Euroopan yhteisön sisävesillä annetun direktiivin (2005/44/EY) nojalla. EU:n sisävesisääntelyä Suomessa sovelletaan vain rajatusti. (LVM, 2021, s. 6) Saimaan kanavaa ei ole määritetty Keski-Euroopassa yleisesti tarjottavien jokitiedotuspalveluiden (RIS) alueeksi vaan kanavassa kulkevilta aluksien tulee täyttää RIS-liikennettä korkeammat SOLAS-vaatimukset. (Liikennevirasto, 2016) Koska Suomi ei sovella sisävesillään jokitiedos-

[7] Säädöksen suomenkielisessä versiossa puhutaan oleellisesta palvelusta. Englanninkielisen kieliversiossa taas 'essential service' eli keskeisestä palvelusta. Suomenkielisessä käännöksessä vaikuttaa olevan käännösvirhe ja tosiasiallisesti on pyritty tarkoittamaan NIS-direktiivin mukaista keskeistä palvelua.

tuspalveluita koskevaa direktiiviä, komission täytäntöönpanoasetus ECDIS-merikarttajärjestelmän pitämisestä yhteiskunnan keskeisenä palveluna ei velvoita Suomea. Tältä osin tilanne on ristiriitainen, koska ruorimerkityn painetun merikartan voi korvata ECDIS-navigointijärjestelmällä Suomessa, mikäli ECDIS-järjestelmässä käytetään virallisia, standardoituja ENC-kartta-aineistoja. (Liikenne- ja viestintäviraston määräys alusten navigointilaitteista ja järjestelmistä, 2012) Mikäli Suomi tulevaisuudessa päätyisi pitämään sisävesien tai koko Suomen talousalueen osalta ECDIS-järjestelmää yhteiskunnan keskeisenä palveluna, ongelmaksi syntyisi valvonnan riippumattomuus. Tällä hetkellä Liikenne- ja viestintävirasto Traficom on verkko- ja tietojärjestelmien turvavelvoitteiden osalta toimivaltainen valvontaviranomainen liikennesektorilla, mutta Traficom myös tuottaa virallisia elektronisia merikarttoja Suomessa, jotka jaetaan jälleenmyyjille Norjassa sijaitsevan PRIMAR-jakelukeskuksen kautta. (Traficom, 2020a) Mikäli Suomessa ECDIS-merikartta-aineiston tuottamista päädyttäisiin pitämään yhteiskunnan keskeisenä palveluna, Traficomiin kohdistuva tietoturvavelvoitteiden valvonta tulisi järjestää uskottavalla ja hallinnollisesti riippumattomalla tavalla ensisijaisesti Traficomin organisaatiorakenteen ulkopuolelle tai vähintään organisatorisesti Traficomin Liikennejärjestelmäpalveluiden ulkopuolelle. ECDIS-karttajärjestelmän sisältämän tiedon tuottamisen lisäksi on syytä tiedostaa, että Suomessa on myös ECDIS-järjestelmien valmistamistoimintaa. Mikäli verkko- ja tietojärjestelmien turvavelvoitteita Suomessa ulotettaisiin elektronisiin merikarttoihin, samalla tulisi arvioida, että tulisiko sääntely mahdollisesti ulottaa myös Furuno Finland Oy:n kaltaiseen yritykseen, joka on ensimmäisten joukossa valmistanut tyyppihyväksytyn ECDIS-karttalaitteen. (Furuno)

Toinen EU:n komission NIS-direktiiviin vesiliikennettä koskevaan soveltamiseen liittyvä täydennys koskee alusten paikannus- ja seurantajärjestelmiä. Kuten edellä ECDIS-järjestelmän osalta, myös tämä täytäntöönpanoasetus liittyy jokitiedotuspalveluin (RIS) soveltamisalaan EU:n sisävesillä. Komission täytäntöönpanoasetuksen mukaan alusten paikannus- ja seurantajärjestelmiin sovelletaan NIS-direktiivin säädöksiä silloin kun ne tarjoavat keskeisiä palveluita. (Komission täytäntöönpanoasetus (EU) 2019/838, alusten paikannus- ja seurantajärjestelmiä koskevista teknisistä eritelmistä ja asetuksen (EY) N:o 415/2007 kumoamisesta, liite kohta 1.1.) Alusten paikannus ja seurantajärjestelmällä tarkoitetaan em. asetuksen liitteen 1.3.a kohdan mukaan alusten automaattista tunnistusjärjestelmää (Automatic Identification System, AIS) sekä komission asetuksen 414/2007 liitteen kohdan 2.12 mukaisia muita mahdollisia elektronisia alusten ilmoitusjärjestelmiä. Vaikka Suomessa EU:n sisävesisääntelyä sovelletaan vain rajatusti, komission täytäntöönpanoasetus ei tältä osin vaikuta aiheuttavan lainsäädännön muutostarpeita Suomessa. Suomessa Fintraffic Meriliikenteenohjauksella on kattava AIS-maa-asemaverkko, jonka tuottamaa tietoa hyödyntävät viranomaiset, Itämeren rannikkovaltion sekä EU:n jäsenvaltiot. Lisäksi verkon keräämät tiedot kootaan taustajärjestelmään, josta ne välitetään edelleen lähes reaaliajassa avoimen datan rajapintapalvelulle. (Väylävirasto, 2019) Huomioiden että alusliikennepalvelulain 16.5 §:n mukaan VTS-palveluntarjoajaa pidetään yhteiskunnan keskeisen palvelun tarjoajana, Suomen lainsäädännössä myös VTS-

palveluntarjoajan ylläpitämä AIS-maa-asemaverkosto tietojärjestelmineen kuuluu jo kansallisesti verkko- ja tietojärjestelmien turvallisuusvelvoitteiden soveltamisalan piiriin.

Yhteenvetona yhteiskunnan keskeisten palveluiden tarjoajien määrittämisestä Suomen vesiliikennesektorilla voidaan todeta, että verkko- ja tietojärjestelmien turvallisuusvelvoitteita Suomessa sovelletaan Fintraffic Meriliikenteenohjaus Oy:n VTS- eli alusliikennepalveluun AIS-järjestelmään liittyvät palvelut mukaan lukien sekä Turun, Naantalin, Hamina-Kotkan ja Helsingin satamiin. Satamien osalta Suomessa puutteena on, että Suomen suurin tavaraliikennesatama Porvoon Kilpilahdessa sekä Ahvenanmaan satamat jäävät soveltamisalan ulkopuolelle. Kappaleessa tuotiin esille, että varustamot on jätetty Suomessa soveltamisalan ulkopuolelle, mutta ulkopuolelle jättämisen perustelut hallituksen esityksessä eivät vastaa direktiivin vaatimuksia ja toisaalta 2020-luvun pandemian esille nostamat huoltovarmuuskysymykset antavat aihetta arvioida varustamoiden asemaa uudestaan. Mikäli tulevaisuudessa Suomi vähemmän valikoiden soveltaisi EU:n sisävesiä koskevaa sääntelyä, tällöin myös ECDIS-järjestelmän elektronisten merikartta-aineistojen tuotantoprosessi voisi olla syytä sisällyttää verkko- ja tietojärjestelmien turvasääntelyn soveltamisalaan, mutta tämä edellyttäisi tarkempaa pohdintaa, kuinka soveltamisen valvonta järjestettäisiin Traficomin ollessa ECDIS-järjestelmän käyttämän kartta-aineiston tuottaja.

2.1.3 Tieliikenteen keskeisten palveluiden tarjoajien määrittely

Suomessa tieliikenteen ohjaus- ja hallintapalveluiden tarjoajan sekä älykkään liikennejärjestelmän ylläpitäjän on huolehdittava verkko- ja tietojärjestelmien suojaamisesta eli NIS-direktiiviä sovelletaan tieliikenteessä näihin kahteen tieliikenteen osa-alueeseen (Laki liikenteen palveluista 140 ja 161 §).

Tieliikenteen ohjaus- ja hallintapalveluilla tarkoitetaan tieliikenteen ohjausta, hallintaa ja varmistusta. Palvelulle on ominaista vuorovaikutus liikenteen kanssa ja reagointi muuttuviin liikennetilanteisiin (Laki liikenteen palveluista 2 § kohta 10). Käytännössä tieliikenteen ohjaus- ja hallintapalveluissa on kysymys Fintraffic Tie Oy:n tarjoamista palveluista, joihin kuuluvat muun muassa tieliikennekeskukset, tunneleiden tekniset järjestelmät, maanteiden muuttuvat opasteet, tiesääjärjestelmät, avoimena datana tarjottavat tieliikenteen olosuhdepalvelut sekä näihin liittyvät tietoliikenne- ja tietotekniset palvelut. (Fintraffic, 2022a) Tietoliikenne- ja tietoteknisiä palveluista esimerkkinä on hälytysajoneuvoille luotava liikennevalojen etuusjärjestelmä (HALI). (Fintraffic, 2022b)

Tieliikenteen ohjaus- ja hallintapalveluiden osalta on mielenkiintoista, että niiden suhdetta NIS-direktiiviin on arvioitu kolmessa eri hallituksen esityksessä. Vuonna 2016 hallituksen esityksessä liikennekaareksi ja siihen liittyviksi laeiksi tunnistettiin tuolloin komission esityksenä olleen NIS-direktiiviehdotuksen vaikutus tieliikenteeseen ja todettiin, että jatkossa liikennepalvelut on suunniteltava tietoturva ja tietosuoja sisäänrakennettuna (security and privacy by design). (HE 161/2016 vp, s. 60) NIS-direktiivin täytäntöönpanoa koskevassa hallituksen esityksessä tieliikenteen ohjaus- ja hallintapalveluita ei pidetty yhteiskunnan kes-

keisenä palveluna. (HE 192/2017 vp, s. 47) Kuitenkin NIS-direktiivin täytäntöönpanoa koskevan hallituksen esityksen ollessa vielä eduskunnan käsiteltävänä, eduskunnalle annettiin uusi hallituksen esitys koskien liikenteenohjauspalveluiden yhtiöittämistä. Tässä hallituksen esityksessä näkökulma oli merkittävästi muuttunut ja tieliikenteen ohjaus- ja hallintapalveluita pidettiin yhteiskunnan keskeisenä palveluna. (HE 34/2018 vp, s. 85) Kahdessa viimeksi mainitussa hallituksen esityksessä liikenteenohjauspalveluita yleensä pidettiin liikennejärjestelmän toimivuuden kannalta keskeisinä, liikenteenohjauksen välitön vaikutus liikenneturvallisuuteen tuotiin esille ja korostettiin, että häiriöt liikenteenohjauksessa johtaisivat liikenneturvallisuuden vaarantumiseen. Erona näissä kahdessa hallituksen esityksessä kuitenkin oli näkökulma verkko- ja tietojärjestelmien merkitykseen tieliikenteen ohjaamisessa. NIS-direktiivin täytäntöönpanoa koskevassa hallituksen esityksessä näkökulmaa voisi kuvailla menneisyyteen ja nykyhetkeen rajoittuneeksi. Siinä älykkään automaation yleistymisen merkitys liikenteenohjauspalveluille tiedostettiin, mutta tieliikenteen ohjauspalvelut rajattiin soveltamisalan ulkopuolelle, koska liikennemerkeillä tai tiemerkinnöillä on keskeinen rooli liikenteen ohjauksessa ja nämä eivät pääsääntöisesti ole riippuvaisia verkko- ja tietojärjestelmistä. (HE 192/2017 vp, s. 47) Tässä yhteydessä on hyvä muistaa, että riippuvuus verkko- ja tietojärjestelmistä on NIS-direktiivin mukainen edellytys, että palvelua voitaisiin direktiivin näkökulmasta pitää yhteiskunnan kannalta keskeisenä. Kuitenkin neljä kuukautta NIS-direktiivin täytäntöönpanoa koskevan hallituksen esityksen antamisen jälkeen toisessa hallituksen esityksessä näkökulma vaihtui tulevaisuuteen katsovaksi ja tieliikenteen ohjaus- ja hallintapalvelut sisällytettiin verkko- ja tietojärjestelmien turvallisuusvelvoitteiden soveltamisalaan kolmesta syystä. Ensimmäinen syy oli, että liikennevälineet ja liikenneinfrastruktuuri ovat kasvavasti riippuvaisia viestintäverkkojen ja tietojärjestelmien luotettavasta toiminnasta. Toiseksi liikenteenohjaus ja hallinta tapahtuvat jatkossa verkkojen ja tietojärjestelmien välityksellä. Kolmanneksi liikenteen ohjauksella on merkittävä rooli liikennejärjestelmän toiminnan ja turvallisuuden kannalta. (HE 34/2018 vp, s. 85)

Toisena yhteiskunnan keskeisenä palveluna tieliikenteen alalla ovat älykkäiden liikennejärjestelmien ylläpitäjät (Laki liikenteen palveluista 161 §), joilla tarkoitetaan ITS-direktiivin (Euroopan parlamentin ja neuvoston direktiivi 2010/40/EU tieliikenteen älykkäiden liikennejärjestelmien käyttöönoton sekä tieliikenteen ja muiden liikennemuotojen rajapintojen puitteista) mukaisia älykkäitä liikennejärjestelmiä. Hallituksen esityksen mukaan liikenneinfrastruktuurin hallinta on lähtökohtaisesti keskeisen palvelun tarjoamista. Tieinfrastruktuuri kuuluu liikenneinfrastruktuuriin, mutta tältä osin vain ITS-direktiivin mukaisten ITS-järjestelmien ylläpitäminen on yhteiskunnan keskeinen palvelu. NIS-direktiiviä kansallisesti täytäntöön pantaessa hallituksen esityksen mukaan ITS-järjestelmiä olivat Hätäkeskuslaitoksen ylläpitämä eCall-hätäpuhelujärjestelmä sekä tuolloin Liikenneviraston ylläpitämät Digiroad -väylätietopalvelu ja Digitraffic -liikennetietopalvelu. (HE 192/2017 vp, s. 48)

Vaikuttaisi siltä, että sekä laki liikenteen palveluista että NIS-direktiivi määrittelevät tieliikenteen älykkäiden liikennejärjestelmien tarjoajat selkeästi laajemmin verkko- ja tietojärjestelmien turvallisuussääntelyn piiriin, mitä Liikenne- ja viestintävirasto Traficom valvovana viranomaisena lakia tulkitsee. NIS-direktiivin liitteen mukaan ITS-direktiivin mukaiset älykkäiden liikennejärjestelmien ylläpitäjät lähtökohtaisesti kuuluvat direktiivin soveltamisalaan. NIS-direktiivin täytäntöönpanoa koskevassa hallituksen esityksessä kolme älykästä liikennejärjestelmää nimenomaisesti nimettiin, liikenteen palveluista annetun lain 161 §:n koskee sanamuodon mukaisesti älykkään liikennejärjestelmän ylläpitäjää ja liikenteen palveluista annetun lain soveltamisalana ovat Suomessa toimipaikan omaavat palveluntarjoajat (Laki liikenteen palveluista 1.2 §). Tästä huolimatta Liikenne- ja viestintävirasto Traficomin mukaan sääntely koskisi vain tieliikennekeskusta liikenteenohjausyhtiönä. (Kyberturvallisuuskeskus, 2021) Vaikuttaisi siis siltä, että lähes neljän vuoden aikana, kun lakia on sovellettu, Traficom ei ole huomioinut älykkäiden liikennejärjestelmien tarjoamista osana verkko- ja tietojärjestelmien turvallisuussääntelyn valvontaa. Seuraavaksi käsittelen tarkemmin kolmea hallituksen esityksessä mainittua älykästä liikennejärjestelmää. Näiden osalta kartoitetaan minkälaista yhteiskunnan toiminnan kannalta keskeistä palvelua ne tarjoavat ja kuka palvelun tarjoajana vastaa verkko- ja tietojärjestelmien turvallisuusvelvoitteista.

Ajoneuvojen hätäpuhelujärjestelmä (eCall) koostuu ajoneuvolaitteesta, viestintäverkosta ja hätäkeskuksissa toteutetusta eCall toiminnallisuudesta. (Viestintävirasto, 2016b) Sisäministeriön hallinnonalaan kuuluvan Hätäkeskuslaitoksen ylläpitämällä eCall-hätäviestipalvelulla tarkoitetaan 31.3.2018 jälkeen EU-alueella tyyppihyväksytyissä henkilö- ja pakettiautoissa pakollisena olevaa eCall-laitetta, joka onnettomuustilanteessa manuaalisesti tai automaattisesti muodostaa yhteyden puhelinvaihteeseen, välittää hätäkeskukselle datapakettina muun muassa ajoneuvon tyyppitiedot, sijainnin ja kulkusuunnan sekä muodostaa puheyhteyden ajoneuvon ja hätäkeskuksen välille. (Traficom, 2020b ja Hätäkeskuslaitos, 2020) Teleyritysten velvollisuutena on huolehtia eCall puhelun yhteydessä päätelaitteelta saatu eCall-ilmaisintieto välitetään hätäpuhelun yhteydessä. (Viestintävirasto, 2016a) Ajoneuvolaitteisiin liittyen Euroopan parlamentin ja neuvoston asetuksen hätänumeroon 112 perustuvan ajoneuvoon asennettavan eCall-järjestelmän käyttöönottoa koskevista tyyppihyväksyntävaatimuksista ja direktiivin 2007/46/EY muuttamisesta (eCall-asetus) artikla 3 määritelmien mukaan eCall-hätäpuhelut voivat olla myös kolmannen osapuolen tukemia hätäpuheluita. Kolmannen osapuolen tukemilla palveluilla tarkoitetaan esimerkiksi yksityisen palveluntarjoajan toteuttamia eCall-palveluita, joissa hätäpuhelun toteuttamisen tai välittämisen lisäksi tarjotaan lisäarvopalveluita. (YourEurope, 2021)

Laki liikenteen palveluista 161 §:n sanamuodon mukaisen tulkinnan mukaisesti on perusteltua, että Hätäkeskuslaitosta eCall-järjestelmän ylläpitäjänä pidetään älykkään liikennejärjestelmän ylläpitäjänä ja siten verkko- ja tietojärjestelmien turvallisuusvelvoitteita tulisi soveltaa tähän osaan Hätäkeskuslaitoksen toiminnasta. Teleyrityksillä on eCall-järjestelmään liittyviä velvollisuuksia,

mutta niiden voi katsoa jäävän tässä yhteydessä pykälän soveltamisalan ulkopuolelle, koska ne eivät ole varsinaisen järjestelmän ylläpitäjiä. Pykälän soveltamisalan määrittämisen osalta kiperin kysymys on, sovelletaanko pykälää eCall-hätäpuheluita välittäviin yksityisiin palveluntarjoajiin. Tämän tutkimuksen puitteissa ei ole mahdollista perehtyä eri ajoneuvovalmistajien ja heidän mahdollisten sopimuskumppaneiden tapaan toteuttaa eCall-hätäpuhelut. Mikäli yksityinen palveluntarjoaja ottaa eCall-hätäpuhelun vastaan tarjoten lisäarvopalvelua eikä vain teleoperaattoriin rinnastettavalla tavalla automaattisesti vain välitä sitä hätäkeskukselle, tällöin palveluntarjoajaa tulisi pitää älykkään liikennejärjestelmän ylläpitäjä ja siten sen Suomen toimintoihin sovellettaisiin NIS-direktiiviin perustuvia velvoitteita liikenteen palveluista annetun lain 161 §:n mukaisesti.

Älykkäinä liikennejärjestelminä NIS-direktiivin täytäntöönpanoa koskevassa hallituksen esityksessä mainittiin myös tuolloisen Liikenneviraston ylläpitämät Digiroad -väylätietopalvelu ja Digitraffic -liikennetietopalvelu. Digiroad -väylätietopalvelussa on kyse Suomen tie- ja katuverkon keskilinjageometrian sekä tärkeimpiä ominaisuustietoja jakavasta avoimen datan tietojärjestelmästä. Väylävirasto omistaa ja vastaa Digiroad -palvelusta ja palvelun operaattorina ja järjestelmän pääkäyttäjänä toimii CGI Suomi Oy. (Väylävirasto, päiväämätön) Nykyisin Digitraffic -liikennetietopalvelua ylläpitää Fintraffic. Digitraffic palvelussa on kyse ajantasaisen avoimen liikennetiedon jakamisesta sovelluskehitykseen Suomen tie-, rautatie- ja vesiliikenteestä. (Fintraffic, 2022c) Digiroad ja Digitraffic -palveluiden osalta on selkeää, että Väylävirasto ja Fintraffic tahoillansa ovat näiden älykkäiden liikennejärjestelmien ylläpitäjiä ja siten verkko- ja tietojärjestelmien turvallisuusvelvoitteiden tulisi kohdistua näihin toimijoihin. Sen sijaan palvelujen verkkosivuilta saatavilla olevien tietojen perusteella vaikuttaisi siltä, että verkko- ja tietojärjestelmien turvallisuusvelvoitteet eivät lakina suoraan velvoita Digiroad -palvelua operoivaa CGI Suomi Oy:tä vaan lakiin perustuvat velvoitteet kohdistuvat vain Väylävirastoon. Luonnollisesti on kuitenkin mahdollista, että Väyläviraston ja CGI Suomi Oy:n välisissä sopimuksissa näiden velvoitteiden sisällön toteuttamisesta on mahdollista tarkemmin sopia.

NIS-direktiivin täytäntöönpano Suomen tieliikennesektorilla vaikuttaa toteutetun NIS-direktiivin liitteessä esitetyn soveltamisalan mukaisesti eikä tutkimusta tehdessä ole tullut esiin erityisiä direktiivitason ja kansallisen tason välisiä kysymyksiä poikkeavista sääntelyn soveltamisaloista. NIS-direktiivissä tieliikenteen keskeiset toimijat on jaettu direktiivin liitteessä kahteen kategoriaan: Liikenteenhallinnasta vastaavat tieviranomaiset ja älykkäiden liikennejärjestelmien ylläpitäjät. Liikenteenhallinnasta vastaavilla tieviranomaisilla tarkoitetaan viranomaista, joka vastaa alueelliseen toimivaltaansa kuuluvien teiden suunnittelusta, valvonnasta ja hallinnoinnista. (Komission delegoitu asetus (EU) 2015/962, Euroopan parlamentin ja neuvoston direktiivin 2010/40/EU täydentämisestä EU:n laajuisten tosiaikaisten liikennetietopalvelujen tarjoamisen osalta, 2(12) artikla) Toisen tieliikenteen keskeisten toimijoiden kategorian muodostaa älykkäiden liikennejärjestelmien ylläpitäjät. Älykkäillä liikennejärjestelmillä tarkoitetaan ITS-direktiivin mukaan tieto- ja viestintäteknologiaa tieliikenteen, liikenteen hallin-

nan ja liikkuvuuden hallinnan aloilla soveltavia järjestelmiä sekä näiden järjestelmien rajapintoja. Tieliikenteen alaan tässä yhteydessä kuulu niin infrastruktuuri, ajoneuvot ja käyttäjät.

Yhteenvetona yhteiskunnan keskeisten palveluiden tarjoajien määrittämisestä Suomen tieliikennesektorilla voidaan todeta, että verkko- ja tietojärjestelmien turvallisuusvelvoitteita Suomessa sovelletaan tieliikenteen liikenteenohjauspalvelun tarjoajaan, joka tällä hetkellä on Fintraffic Tie Oy. Traficomin nykyisestä soveltamiskäytännöstä poiketen tutkimuksessa esitetään, että sääntely koskee älykkäiden liikennejärjestelmien osalta myös Hätäkeskuslaitosta eCall-järjestelmän hätäpuheluiden vastaanottamisen osalta sekä niitä Suomen oikeudenkäytön piirissä olevia yksityisiä palveluntarjoajia, jotka tekevät enemmän kuin vain automaattisesti välittävät eCall-hätäpuheluita Suomen Hätäkeskuslaitokselle. Lisäksi soveltamisalaan nykyisestä soveltamiskäytännöstä poiketen sisältyy Väylävirasto Digiroad-palvelun ylläpitäjänä sekä Fintraffic Digitraffic-palvelun ylläpitäjänä. Fintrafficin osalta velvoitteiden täsmällinen kohdentaminen riippuu yrityksen organisaatiorakenteesta ja erityisesti siitä, toteutetaanko Digitraffic palvelu Fintraffic Tie Oy:n organisaatiossa vai onko kyseessä Liikenteenohjausyhtiö Fintraffic Oy:n konsernitason palvelu.

2.2 Keskeisten palveluiden tarjoajien velvollisuudet

Kappaleen tarkoituksena on vastata kysymykseen, mitä sääntelyn kohteena olevilta toimijoilta vaaditaan NIS-direktiivin pohjalta annetun kansallisen sääntelyn mukaan. Aihepiiriä koskevassa kirjallisuudessa aiheesta saatetaan käyttää käsitteitä vähimmäisvaatimukset, compliance -vaatimukset tai lakiin perustuvat velvollisuudet. Näiden käsitteiden ongelmana on, että käsitteiden sisältöä ei välttämättä ymmärretä samalla tavalla ja niiden sisältö voi poiketa EU-oikeuden ja kansallisen oikeuden tasoilla. Tässä tutkielmassa käytetään käsitettä vähimmäisvaatimukset, kun kyseessä on EU-oikeus ja NIS-direktiivistä jäsenvaltioille ilmenevät vaatimukset (EU-oikeuden ja jäsenvaltion välinen suhde). Käsitettä lakiin perustuvat velvollisuudet tai lyhyesti vain velvollisuudet käytetään, kun käsitellään mitä Suomen kansallisen lainsäädännön mukaan vaaditaan edellä kappaleessa 2.1 tunnistetuilta liikennejärjestelmän keskeisten palveluiden tarjoajilta (kansallisen lainsäädännön ja oikeushenkilön välinen suhde). Toimijoihin kohdistuvien velvollisuuksien osalta otan lähempään tarkasteluun erityisesti riskienhallinnan ja ilmoittamisvelvollisuuden, joita käsitellään erillisinä alakappaleina. Vastauksen antaminen kysymykseen, minkälaista (tietoturva)riskienhallintaa toimijoilta vaaditaan, edellyttää tutkimuksessa selvitettävän, minkä tietoturvallisuudesta toimijoiden tulee varmistua, miten tietoturvallisuudesta tulisi varmistua ja onko olemassa jokin vähimmäistaso, mikä toimijoiden tulisi täyttää. Riskienhallinnan osalta myös selvitetään, kuinka tarkasti toimijoiden tulisi dokumentoida riskienhallintansa. Tietoturvapoikkeamien ilmoittamisvelvollisuuden osalta selvitetään, että mistä tietoturvapoikkeamista toimijoiden tulisi ilmoit-

taa. Ilmoitusvelvollisuutta koskevaan kysymykseen vastaaminen edellyttää selvitettävän, mitä tarkoitetaan merkittävällä tietoturvapoikkeamalla. Kun kansallisen lainsäädännön riskienhallinta ja ilmoittamisvelvollisuuden kokonaisuus on käyty läpi, pystytään muotoilemaan vastaus kysymykseen, vastaako kansallisessa lainsäädännössä asetetut vaatimukset direktiivin riskienhallinnan ja ilmoittamisvelvollisuuden vähimmäistavoitetta.

2.2.1 Riskienhallintavelvollisuus

Liikennejärjestelmän toimijoihin kohdistuvat NIS-direktiivin kansalliseen täytäntöönpanoon perustuvat riskienhallintavelvollisuudet löytyvät sektorikohtaisesta lainsäädännöstä. Tämä tarkoittaa, että kutakin liikkumismuotoa koskevat velvollisuudet löytyvät yhdestä tai useammasta kyseistä liikkumismuotoa koskevasta erityislaista. Eri toimijoita koskevat sektorikohtaiset riskienhallintavelvollisuudet esitetään kootusti alla olevassa taulukossa. Taulukossa on alleviivattuna ne kohdat, jotka ylittävät kaikille sektoreille yhteisen vähimmäistason.

TAULUKKO 1 Velvoitteet riskien hallitsemiseksi

Toimija	Laki	Hallituksen esityksen rajaus	Hallituksen esityksen vähimmäistaso
Tieliikenteen ohjaus- ja hallintapalvelun tarjoajan	on huolehdittava käyttämiinsä liikenteen turvallisuuden kannalta merkittäviin viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. (Laki liikenteen palveluista 140.1 §)	Riskienhallintavelvoite koskisi vain viestintäverkkoja ja tietojärjestelmiä, jotka olisivat liikenneturvallisuuden kannalta merkittäviä. (HE 34/2018 vp, s. 86)	Liikenneturvallisuuden kannalta merkittävinä olisi ainakin pidettävä järjestelmiä, jotka ovat palvelun tarjonnan jatkuvuuden kannalta keskeisiä tai joihin kohdistuvat häiriöt voisivat aiheuttaa riskin tieliikenteen turvallisuudelle. (HE 34/2018 vp, s. 86)
Älykkään liikennejärjestelmän ylläpitäjän	on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. (Laki liikenteen palveluista 161.1 §)	Riskienhallintavelvoite koskisi vain viestintäverkkoja ja tietojärjestelmiä, jotka olisivat älykkään liikennejärjestelmän turvallisuudelle merkittäviä. (HE 192/2017 vp, s. 76)	Älykkään liikennejärjestelmän turvallisuuden kannalta merkittävinä olisi ainakin pidettävä järjestelmiä, jotka ovat palvelun tarjonnan jatkuvuuden kannalta keskeisiä. (HE 192/2017 vp, s. 76)
Valtion rataverkon haltijan sekä liikenteenohjauspalvelun tarjoajan	on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. (Raideliikennelaki 169.1 §)	Riskienhallintavelvoite koskisi vain viestintäverkkoja ja tietojärjestelmiä, jotka olisivat rautatieliikenteen turvallisuuden kannalta merkittäviä. (HE 192/2017 vp, s. 70)	Rautatieliikenteen turvallisuuden kannalta merkittävinä olisi ainakin pidettävä järjestelmiä, jotka ovat palvelun tarjonnan jatkuvuuden kannalta keskeisiä tai joihin kohdistuvat häiriöt voisivat aiheuttaa riskin rautatiejärjestelmän turvallisuudelle. (HE 192/2017 vp, s. 70)
VTS-palveluntarjoajan	on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. (Alusliikennepalvelulaki 16.5 §)	Riskienhallintavelvoite koskisi vain viestintäverkkoja ja tietojärjestelmiä, jotka olisivat merenkulun turvallisuuden kannalta merkittäviä. Velvoite kohdistuisi VTS-palveluntarjoajan tehtäviin, jotka liittyvät liikenteenohjaamisen operatiiviseen toimintaan. (HE 192/2017 vp, s. 71)	Merenkulun turvallisuuden kannalta merkittävinä olisi ainakin pidettävä järjestelmiä, jotka ovat palvelun tarjonnan jatkuvuuden kannalta keskeisiä tai joihin kohdistuvat häiriöt voisivat aiheuttaa riskin merenkulun turvallisuudelle. (HE 192/2017 vp, s. 71)
Yhteiskunnan toiminnan kannalta merkittävän satamanpitäjä	on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. (Turvatoimilaki 7 f.1 §)	Riskienhallintavelvoite koskisi vain viestintäverkkoja ja tietojärjestelmiä, jotka olisivat merenkulun turvallisuuden kannalta merkittäviä. (HE 192/2017 vp, s. 73)	Merenkulun turvallisuuden kannalta merkittävinä olisi ainakin pidettävä järjestelmiä, jotka ovat palvelun tarjonnan jatkuvuuden kannalta keskeisiä tai joihin kohdistuvat häiriöt voisivat aiheuttaa riskin merenkulun turvallisuudelle. (HE 192/2017 vp, s. 73)

Taulukosta ilmenee, että kaikilla soveltamisalan piiriin kuuluvilla toimijoilla on velvollisuus huolehtia käyttämiinsä viestintäverkkoihin ja tietotojärjestelmiin kohdistuvien riskien hallinnasta. Ainoastaan tieliikenteen ohjaus- ja hallintapalvelun tarjoajan osalta riskienhallintavelvoitteen laajuutta on pykälätasolla kavennettu tarkentamalla velvollisuuden koskevan vain liikenteen turvallisuuden kannalta merkittäviin viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallintaa. Huomioiden kuitenkin, että älykkäiden liikennejärjestelmien, raideliikenteen sekä VTS-palveluiden ja satamien osalta vastaava riskienhallintavelvollisuuden laajuutta kaventava rajaus on tehty hallituksen esityksissä, tieliikenteen ohjaus- ja hallintapalveluihin kohdistuva riskienhallintavelvoite ei pykälän sanamuodosta huolimatta tosiasiallisesti poikkea muista liikennemuodoista. Tästä on tehtävissä johtopäätös, että riskienhallintavelvoite ei koske kaikkia toimijan käyttämiä viestintäverkkoja ja tietojärjestelmiä, vaan vähintään niitä

viestintäverkkoja ja tietojärjestelmiä, jotka ovat kyseisen liikkumismuodon turvallisuudelle merkittäviä.

Kaikille liikennöintimuodoille yhteistä on, että kyseisen liikkumismuodon kannalta merkittävinä olisi ainakin pidettävä järjestelmiä, jotka ovat palvelun tarjonnan jatkuvuuden kannalta keskeisiä. Hallituksen esityksessä ja NIS-direktiivissä ei tarkemmin määritellä, mitä jatkuvuudella tarkoitetaan. Suomen kielessä Turvallisuuskomitean mukaan jatkuvuudenhallinnalla tarkoitetaan organisaation ylimmän johdon hyväksymää strategista ja operatiivista toimintaa, jolla organisaatio varautuu hallitsemaan häiriötilanteet ja jatkamaan toimintaa ennalta määritellyllä hyväksyttävällä tasolla. (Sanastokeskus TSK, 2017) Traficom valvovana viranomaisena käyttää käsitettä toimintavarmuus synonyyminä jatkuvuuden ja häiriötilanteiden hallinnalle. Riskienhallinnan piiriin tällöin tulisi katsoa kuuluvan kaikki ne viestintäverkot ja tietojärjestelmät, jotka ovat keskeisiä toiminnan palvelun tarjoamisen jatkuvuuden ja häiriötilanteiden hallinnan kannalta. (Traficom, 2021c)

Tieliikenteen ohjauspalveluiden, raideliikenteen, meriliikenteen ohjauspalveluiden ja satamien kohdalla viestintäverkkojen ja tietojärjestelmien riskienhallintavelvoite koskisi aina myös järjestelmiä, joihin kohdistuvat häiriöt voisivat aiheuttaa riskin kyseisen liikkumismuodon turvallisuudelle. Hallituksen esityksen mukaan riskillä tarkoitetaan mitä tahansa kohtuullisesti tunnistettavissa olevaa tilannetta tai tapahtumaa, joka saattaa vaikuttaa haitallisesti viestintäverkkojen ja tietojärjestelmien turvallisuuteen. (HE 192/2017 vp, s. 70, 71, 74 ja 76) Kirjaus vaikuttaisi aiheuttavan käsitteellisen ristiriidan riskienhallinnan kohteessa. Toisaalta riskienhallinnan kohteena ovat järjestelmät, jotka ovat turvallisuuden kannalta merkittäviä. Toisaalta turvallisuuden kannalta merkittävinä olisi ainakin pidettävä järjestelmiä, joiden häiriö voi aiheuttaa turvallisuudelle riskin. Hallituksen esityksessä ei määritetä tasoa riskin suuruudelle tai kuinka riskiä tulisi mitata. Tästä voidaan täten tehdä johtopäätös, että riskienhallintavelvoite koskee kaikkia järjestelmiä, jotka voivat aiheuttaa minkä tasoisen riskin tahansa kyseisen liikennöintimuodon turvallisuudelle.

Lisäksi taulukosta havaitaan, että hallituksen esityksen tasolla VTS-palveluntarjoajaan kohdistuva riskienhallintavelvoitteen laajuutta on kavennettu aavistus muita liikennemuotoja enemmän. VTS-palveluiden osalta riskienhallintavelvoite koskee vain liikenteenohjaamisen operatiiviseen toimintaan käytettäviä viestintäverkkoja ja tietojärjestelmiä. Rajauksen tosiasiallinen merkitys lienee vähäinen, mutta tarkoituksena on selkeästi ollut rajata hallinnolliset tehtävät sekä hallinnolliset viestintäverkot ja tietojärjestelmät riskienhallintavelvoitteen ulkopuolelle siinä määrin, kun ne eivät liity operatiivisten toimintojen hoitamiseen. Hallituksen esityksen kirjausta voidaan tulkinta niin, että mikäli operatiiviseen liikenteenohjaukseen käytettävät viestintäverkot ja tietojärjestelmät eivät ole selkeästi erotettu muista mahdollisista hallinnollisista verkoista ja järjestelmistä ja ne toimivat samassa ympäristössä, tällöin riskienhallintavelvoite koskee koko tietoliikenne- ja tietojärjestelmäympäristöä. Tulkinta on perusteltu, koska riskienhallintavelvollisuus menetettäisi merkityksensä, mikäli hallinnolliset järjes-

telmät eivät kuuluisi riskienhallinnan piiriin ja hallinnollisen järjestelmän tietoturvahaavoittuvuutta hyväksikäyttäen olisi mahdollista vaikuttaa operatiivisten viestintäverkkojen ja tietojärjestelmien toimintaan (hyökkääjän siirtyminen järjestelmien välille eli niin sanottu lateraali liikkuminen).

Tässä yhteydessä on myös syytä tuoda esille yksi sektorikohtaisen sääntelyn heikkous. Hallituksen esityksessä käytetyt sanamuodot ovat ongelmallisia liikennejärjestelmän kokonaisuuden näkökulmasta ja tuovat esille sektorikohtaisen sääntelyn heikkoudet siltä osin, kun sääntely ei huomioi liikkumismuotojen rajapintoja. Esimerkiksi satamien verkko- ja tietojärjestelmien turvallisuuden riskienhallinta ei vaikuttaisi ulottuvan sataman alueella tapahtuvan raideliikenteen turvallisuuteen tai jatkuvuuteen eikä raideliikenteen verkko- ja tietojärjestelmien turvallisuuden riskienhallintavelvoite ulottuisi tie- tai meriliikenteen turvallisuuteen tai jatkuvuuteen, mikäli kyse ei samalla olisi sellaisesta riskistä, jonka hallitseminen vaikuttaisi merkittävästi kyseisen liikkumismuodon turvallisuuteen tai kyseisen liikkumismuodon itsensä jatkuvuuteen. Käytännön elämässä ongelma voi kaventua lähinnä teoreettiseksi, mutta sääntelyä kehitettäessä voisi olla koko yhteiskunnan häiriösietoisuuden varmistamin näkökulmasta parempi, että turvallisuuden vaarantamista tai jatkuvuutta ei kytkettäisi yksittäisen liikkumismuotoon vaan koko logistiikkaketjuun tai laajemmin kaikkiin yhteiskunnan keskeisiin palveluihin.

Lainsäädännön ja lain esitöiden perusteella toimijan käyttämien viestintäverkkojen ja tietojärjestelmien riskienhallintavelvollisuuden laajuus määrittyy jatkuvuudenhallinnan, turvallisuuteen kohdistuvan riskin, turvallisuuden kannalta merkittävyyden sekä operatiivisen toiminnan käsitteiden kautta. Edellä luetelluista käsitteistä voi korostaa käsitteen jatkuvuudenhallinta merkitystä riskienhallintavelvollisuuden laajuuden määrittämisessä, koska se on yhteinen kriteeri kaikille käsitellyille liikennöintimuodoille ja käsitteenä laajin eli yksittäinen käsite kattaa suuren osan toimijan viestintäverkoista ja tietojärjestelmistä. Edellä esitetyn perusteella voidaan yhteenvetona todeta, että riskienhallintavelvollisuuden kohteena ovat kaikki toimijan käyttämät viestintäverkot ja tietojärjestelmät,

1. jotka ovat kyseisen palvelun tarjoamisen jatkuvuuden tai häiriötilanteiden hallinnan kannalta keskeisiä tai
2. jotka ovat kyseisen liikkumismuodon turvallisuuden kannalta merkittäviä taikka
3. joihin kohdistuvat häiriöt voisivat aiheuttaa riskin kyseisen liikennöintimuodon turvallisuudelle (tie-, raide- ja meriliikenteen ohjaus, valtion rataverkon haltija ja satamat) ja
4. liittyvät liikenteenohjaamisen operatiiviseen toimintaan (meriliikenteenohjaus).

Kun toimija on tunnistanut vähintään edellä mainitut viestintäverkot- ja tietojärjestelmät riskienhallinnan kohteeksi, voidaan edetä määrittämään, mitä riskienhallinnalla tässä yhteydessä tarkoitetaan. NIS-direktiivin täytäntöönpanoa sekä liikenteenohjauksen yhtiöittämistä koskevissa hallituksen esityksissä riskienhal-

linta on määritetty käytännössä sanamuodoltaan identtisellä tavalla. Alla esitetään suora lainaus hallituksen esityksistä. Alleviivatut kohdat ovat kirjoittajan lisäämiä korostuksia ja vastaavat NIS-direktiivin artikloissa käytettyjä sanamuotoja:

> Riskienhallinnalla tarkoitettaisiin asianmukaisia organisatorisia ja teknisiä toimenpiteitä,[8] joilla varmistettaisiin viestintäverkkojen ja tietojärjestelmien kyky suojautua tietyllä varmuudella toimilta, jotka vaarantavat tallennettujen tai siirrettyjen tai käsiteltyjen tietojen taikka muiden kyseisissä järjestelmissä tarjottujen tai niiden välityksellä saatavilla olevien palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden.[9] Riskienhallinnan tulisi sisältää asianmukaiset toimenpiteet, joilla ehkäistään ja minimoidaan palvelujen tarjoamisessa käytettyjen järjestelmien tietoturvallisuuteen liittyvien häiriöiden vaikutus palvelujen jatkuvuuteen.[10] Riskienhallintaan kuuluvia toimenpiteitä voisivat olla esimerkiksi turvallisuussuunnitelmien laatiminen, testaaminen käytännössä tai auditoiminen, tiedon suojaus- ja salaustuotteiden käyttö sekä tiettyjen tunnettujen tietoturvallisuusstandardien, kuten ISO/IEC 27001:2013 -standardin, noudattaminen. Riskillä tarkoitettaisiin mitä tahansa kohtuullisesti tunnistettavissa olevaa tilannetta tai tapahtumaa, joka saattaa vaikuttaa haitallisesti viestintäverkkojen ja tietojärjestelmien turvallisuuteen.[11] Riskienhallinnan tulisi olla todennettavassa muodossa. Dokumentoinnin tavoite on edistää riskien johdonmukaista hallintaa ja toimijan tietoisia ratkaisuja siitä, miten riskien hallitsemiseen tarvittavat toimet mitoitetaan. Dokumentointi mahdollistaisi myös sen, että viranomainen voi tarvittaessa jälkikäteen arvioida pykälän velvoitteiden noudattamista. Dokumentointi voisi tarkoittaa esimerkiksi kirjallisessa muodossa laadittavien riskiarvioiden, turvallisuusohjeiden tai toimintasuunnitelmien laadintaa taikka todistuksia turvallisuustarkastusten suorittamisesta. – –. (HE 192/2017 vp, s. 70, 71, 73, 76 ja HE 34/2018 vp, s. 66)

Koska hallituksen esityksen tekstissä on suurelta osin käytetty NIS-direktiivin sanamuotoja, tässä yhteydessä on syytä verrata, kuinka riskienhallinta ymmärretään direktiivissä.

> Artikla 14.1: 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.
>
> Artikla 14.2: 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.

[8] 14(1) artikla
[9] 4 artikla 2 kohta
[10] 14(2) artikla
[11] 4 artikla 9 kohta

Hallituksen esityksen riskienhallinnan määrittelystä voidaan ensinnäkin todeta, että siinä on suurelta osin käytetty NIS-direktiivin sanamuotoja. Toiseksi voidaan havaita, että hallituksen esityksen esimerkit riskienhallintaan kuuluvista toimenpiteistä sekä riskienhallinnan dokumentoinnin esimerkeistä ovat kansallisia esimerkkejä eli niitä ei ole mainittu direktiivissä. Vaikuttaisi myös siltä, että hallituksen esitys asettaa NIS-direktiivin minimitasoa korkeamman vaatimuksen siinä, että riskienhallinnan tulisi olla kirjallisessa muodossa, mikä mahdollistaisi myös jälkikäteisen arvioinnin velvoitteiden noudattamisesta. Toisaalta Suomen lainsäädäntö ja hallituksen esitys ei huomioi direktiivissä esitettyä vaatimusta huomioida uusin tekniikka riskienhallinnassa.

Riskienhallintavelvollisuuden vähimmäistason määrittämiseksi lähempään tarkasteluun on syytä ottaa ne hallituksen esityksen kohdat, joiden taustalla on direktiivin artiklojen jäsenvaltioita koskevat vähimmäisvaatimukset, joissa kansallisesti asetetaan direktiiviä pidemmälle menevä velvoite sekä kohdat, jotka direktiivissä on kirjoitettu velvoittavaan muotoon, mutta jätetty hallituksen esityksessä mainitsematta. Riskienhallinnan sisällön vähimmäistason käsittely etenee seuraavaksi niin, että ensin selvitetään mitä riskienhallinnan sisältämillä asianmukaisilla ja oikeasuhtaisilla organisatorisilla ja teknisillä toimenpiteillä tarkoitetaan. Tämän jälkeen pyritään määrittämään suuntaviivoja, mitä kyvyllä suojautua tietyllä varmuudella tietoja tai palvelun saatavuutta vaarantavilta toimilta tarkoitetaan. Kolmanneksi tutkitaan, mitä riskin määritelmä tässä yhteydessä vähintään pitää sisällään. Neljäntenä kohtana perehdytään riskienhallinnan dokumentointivelvollisuuden vähimmäistason määrittämiseen ja viidennessä alakappaleessa selvitetään uusimman tekniikan vaatimuksen merkitystä direktiivissä.

2.2.1.1 Asianmukaiset ja oikeasuhtaiset tekniset ja organisatoriset toimenpiteet

Hallituksen esityksen yksityiskohtaisten perusteluiden mukaan riskienhallinnalla tarkoitettaisiin asianmukaisia organisatorisia ja teknisiä toimenpiteitä. Määritelmä poikkeaa direktiivin 14(1) artiklan sanamuodosta siltä osin, että direktiivissä puhutaan asianmukaisista *ja oikeasuhtaisista* teknisistä ja organisatorisista toimenpiteistä (en. appropriate and proportionate technical and organisational measures, sv. ändamålsenliga och proportionella tekniska och organisatoriska åtgärder). Käytännön soveltamisen kannalta suomenkielisen käsitteen asianmukaisuus voidaan tulkita kattavan myös oikeasuhtaisuuden, eikä englanninkielisessä sääntelyssä tyypillistä idiomiparia approriate and proportionate ole välttämätöntä suomen kielessä toistaa.

Direktiivin artiklat eivät tarjoa selvennystä, minkälaisia kriteerejä vasten asianmukaisuutta ja oikeasuhtaisuutta mitataan taikka mitä tekniset ja organisatoriset toimenpiteet merkitsevät. Tulkinta-apua asianmukaisuuden ja oikeasuhtaisuuden määrittämiseen tarjotaan direktiivin johdantotekstin kohdassa 53. Kohdan mukaan riskienhallintavaatimukset eivät saisi aiheuttaa suhteetonta taloudellista ja hallinnollista rasitetta, vaan niiden tulisi olla oikeassa suhteessa riskit ja uusin tekniikka huomioiden. Kohta vaikuttaa kiinnittävän asianmukaisuu-

den ja oikeasuhtaisuuden käytännössä taloudellisiin realiteetteihin eli riskienhallinnan taloudellisiin kustannuksiin ja riskien hallitsemiseen kohdennettaviin resursseihin. Mikäli riski kuvastaa taloudellisen menetyksen ja sen todennäköisyyden suhdetta niin tällöin asianmukaisuuden ja oikeasuhtaisuuden arviointi lienee jossakin määrin mahdollista. Kuitenkin, mikäli riskillä kuvataan ihmisten hengen tai terveyden vahingoittumisen ja todennäköisyyden suhdetta, tällöin asianmukaisuuden ja oikeasuhtaisuuden arviointi ensisijaisesti taloudellisin perustein on kyseenalaista.

Direktiivin johdantotekstistä löytyy myös negatiivinen määritelmä riskienhallintatoimenpiteiden asianmukaisuudelle ja oikeasuhtaisuudelle eli määritelmä siitä, mikä ei ole asianmukaista ja oikeasuhtaista. Direktiivin johdantotekstin kohdan 51 mukaan toimenpiteet eivät saisi edellyttää tietyn kaupallisen tietoja viestintäteknologian suunnittelua, kehittämistä tai valmistamista tietyllä tavalla. Tulkintaohjetta voisi luonnehtia teknologianeutraliteetin periaatteeksi eli sellaiset kansalliset vaatimukset, jotka suoraan tai välillisesti edellyttäisivät jonkin tietyn kaupallisen ratkaisun käyttöä eivät täyttäisi asianmukaisuuden ja oikeasuhtaisuuden vaatimusta. Vastaavasti LVM on korostanut teknologianeutraliteettia osana turvallisuusriskienhallinnan periaatteita. (LVM, 2017, s. 10).

NIS-direktiivin koordinaatioryhmä ei ole suoraan ohjeistanut mitä asianmukaisella ja oikeasuhtaisella tarkoitetaan, mutta koordinaatioryhmä on suosittanut seitsemän periaatteen huomiointia turvallisuustoimenpiteitä harkitessa. Koordinaatioryhmän esittämän periaatteet ovat tehokkuus, tapauskohtaisuus, yhteensopivuus, kohtuullisuus, konkreettisuus, todennettavuus ja kattavuus. Periaatteiden lisäksi ryhmä suosittaa yksityisen ja julkisen sektorin yhteistyötä sekä kustannusten ja hyödyn tasapainottamista. (NIS CG, 2018a, s. 9-10) Kuten edellä on esitetty, käsitteet asianmukaisuus ja oikeasuhtaisuus ovat hyvin monitulkintaisia kriteereitä ja NIS-koordinaatioryhmän useat tulkintaa ohjaavat periaatteet eivät merkittävästi tulkintaa helpota. Tämän johdosta tutkielmassa tyydytään toteamaan, että asianmukaisuuden ja oikeasuhtaisuuden käsite saa sisältönsä viranomaisten tosiasiallisen soveltamiskäytännön ja valvontatoiminnan kautta, tai kuten Iso-Britannian kyberturvallisuuskeskus (National Cyber Security Centre, NCSC) asian muotoilee, heidän toimivaltaan ei kuulu kyberturvallisuuden ja varautumisen tason asianmukaisuuden ja oikeasuhtaisuuden (appropriate and proportionate) arviointi vaan se on toimintaa valvovan tai säätelevän tahon määritettävä. (NCSC UK, 2019)

Riskienhallinnan tekniset ja organisatoriset toimenpiteet ensinnäkin korostavat sitä, että riskienhallinta ei rajoitu tekniseen tietoturvallisuuteen vaan kyse on laajemmasta vaatimuksesta, joka pitää sisällään ihmisiin ja prosesseihin liittyviä toimenpiteitä. Direktiivin johdantotekstin kohta 46 tarjoaa tulkinta-apua vähimmäistoimenpiteiden määrittämiseen. Kohdan mukaan riskienhallintatoimenpiteisiin sisältyvät mahdollisten poikkeamien riskin tunnistaminen, poikkeamien estäminen, havaitseminen ja käsitteleminen sekä poikkeamien vaikutusten lieventäminen. Edellä mainitun listan kaikkiin kohtiin liittyy selkeästi sekä teknisiä että organisatorisia toimenpiteitä. Esimerkiksi uhkien havaitseminen voi vaatia tietoteknisiä ratkaisuja uhkavasta kertovan herätteen antamiseksi, minkä

lisäksi ihmiseltä voidaan vaatia tietokoneen tekemän tunnistuksen todentamista ja tämän jälkeen prosessia eli toimintamallia, kuinka tunnistuksen jälkeen toimitaan.

Johdantotekstin lisäksi tulkinta-apua voidaan saada direktiivin vaatimuksista digitaalisten palveluiden tarjoajille. NIS-direktiivin 16.1 artiklan mukaan digitaalisten palvelun tarjoajien on otettava riskienhallintatoimenpiteissä huomioon seuraavat seikat:

> a) järjestelmien ja tilojen turvallisuus,
> b) poikkeamien käsittely,
> c) liiketoiminnan jatkuvuuden hallinta,
> d) seuranta, tarkastukset ja testaukset ja
> e) kansainvälisten standardien noudattaminen.

Nämä seikat eivät ole suoraan artiklan sanamuodon mukaan sovellettavissa yhteiskunnan keskeisten palveluiden tarjoajiin. Kuitenkin direktiivin johdantotekstin kohdat 57 ja 60 yhdessä luettuina puoltavat tulkintaa, että digitaalisten palveluiden tarjoajiin kohdistettavat vaatimukset olisivat kevyempiä tai vähemmän tiukempia kuin keskeisten palveluiden tarjoajiin kohdistettavat vaatimukset. Mikäli tällainen direktiivin systematiikka koskeva tulkinta hyväksytään, tällöin yhteiskunnan keskeisten palveluiden tarjoajilta voitaisiin analogisesti myös vaatia kyseisten kohtien huomioimista.

Teknisten ja organisatoristen riskienhallintakeinojen vähimmäistasosta ei NIS-direktiivin perusteella vielä voida tehdä kovin pitkälle meneviä johtopäätöksiä, joten tulkinta-apua on syytä hakea muista EU-säädöksistä. EU:n direktiivin 2009/140/EY artikla 13 a(1) sisältää vastaavan kaltaisen velvollisuuden sähköisten viestintäpalveluiden tarjoajille toteuttaa tarvittavat tekniset ja organisatoriset keinot hallitakseen riskejä. Velvoite on Suomessa toteutettu lailla sähköisen viestinnän palveluista. Lakia koskevan hallituksen esitys sisältää esimerkkilistan vaadittavista teknisistä ja organisatorisista toimenpiteistä:

> "[L]aitteiden ja järjestelmien pääsynvalvonta, tietojen ja järjestelmien luvattoman käytön esto, käsittelytapahtumien kirjaaminen, tietoliikenteen alkuperävalvonta ja reititysvalvonta, järjestelmien käyttöoikeuksien määrittely, ylläpitotoimien asianmukainen järjestäminen ja tietojen sekä järjestelmien suojaaminen tietoturvaa vaarantavilta teoilta tai tapahtumilta, kuten viruksilta ja muilta haittaohjelmilta. Lisäksi tietoturvatoimia ovat tietoliikenteen häirinnän valvonta ja sen estäminen." (HE 221/2013 vp, s. 91)

Vastaavasti NIS-direktiivin kanssa suurin piirtein samanaikaisesti valmistellussa ja voimaan tulleessa EU:n tietosuoja-asetuksessa vaaditaan teknisten ja organisatoristen riskienhallintakeinojen käyttöä, joten myös tietosuoja-asetuksen kautta saadaan tulkinta-apua NIS-direktiivin sisällön selvittämiseksi. Tietosuoja-asetuksen 32 artiklan mukaan henkilötietojen käsittelyn turvallisuuden varmistamiseksi ”on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet”. Artiklassa luetellaan myös esimerkkejä toimenpiteistä, joilla riskiin suhteutettu taso voidaan pyrkiä

varmistamaan: Henkilötietojen salaus, kyky ”taata käsittelyjärjestelmä ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus”, kyky palautua fyysisistä ja teknisistä vikatilanteista sekä teknisten ja organisatoristen toimenpiteiden tehokkuuden arviointi. Tietosuojaryhmä WP29:n tulkintaohjeen mukana teknisten ja organisatoristen keinojen keskiössä ovat kyky havaita, vastata ja raportoida tietosuojapoikkeamista kohtuullisessa ajassa. (Tietosuojatyöryhmä WP 29, 2018, s. 13)

Kotimaista oikeuskäytäntöä NIS-direktiivin perusteella annetusta sääntelystä ei ole, mutta tietosuoja-asetuksen teknisten ja organisatoristen keinojen arviointi liittyi oleellisesti tietotosuojavaltuutetun päätökseen 7.12.2021 Vastaamo -tapauksesta. Tietosuojavaltuutetun mukaan tekniset ja organisatoriset keinot edellyttävät tietoisuutta sekä tietojärjestelmien luottamuksellisuuteen, eheyteen, käytettävyyteen ja vikasietoisuuteen vaikuttavista että niitä vaarantavista seikoista. Lisäksi keinot edellyttävät luottamuksellisuuden, eheyden, käytettävyyden ja vikasietoisuuden toteutumisen sekä fyysisten ja teknisten vikatilanteiden aktiivista valvontaa. Kolmanneksi keinot edellyttävät sellaisten menettelyiden käyttämistä, joilla säilytettään tietoisuus käytettyjen toimenpiteiden tehokkuudesta. Tietosuojavaltuutetun päätöksessä korostetaan, että teknisten ja organisatoristen keinojen asianmukaisuus edellyttää tietoisuutta turvallisuuden tason toteutumisesta, eikä tietämättömyydellä turvallisuuden tasosta voida välttää tätä velvollisuutta. Tietosuojavaltuutetun päätöksen mukaan teknisten ja organisatoristen keinojen ei katsottu olleen asianmukaisia, kun Vastaamon tietokantaa ei oltu suojattu palomuurilla, pääkäyttäjätunnusta ei oltu suojattu salasanalla ja kirjautumismahdollisuuksia eri IP-osoitteista ei ollut rajoitettu. (Tietosuojavaltuutettu, 2021)

Tietosuojavaltuutetun Vastaamoa koskevassa päätöksessä tietoturvayritysten havaitsemien puutteiden korjaamista pidettiin asianmukaisena:

> ”Havaitsemiensa puutteiden perusteella Nixu on esittänyt Vastaamolle 17 suositusta korjaaviksi toimenpiteiksi. Nixun mukaan muun ohella potilastietojärjestelmän palvelin tulee suojata palomuurilla siten, että muiden kuin www-palveluiden käyttäminen internetistä on estetty, ylläpitäjillä on oltava henkilökohtaiset tunnukset vahvoilla salasanoilla, pääsy potilastietojärjestelmän palvelimelle on syytä rajata VPN-yhteydellä siten, että palvelin ei ole lainkaan saavutettavissa internetin yli ilman VPN-tunnuksia, palvelimen lokit tulee tallentaa erilliselle lokipalvelimelle vähintään vuoden ajan, potilastietokannan pääkäyttäjätunnuksella kirjautuminen ulkoverkosta tulee estää, tietokanta- ja web-applikaatiopalvelimet on eriytettävä erillisiksi palvelimiksi, joista tietokantapalvelimen yhteydet rajoitetaan vain web-applikaatiopalvelimeen, tietokantapalvelimen ohjelmistoihin on asennettava säännöllisesti uusimmat tietoturvapäivitykset, ja potilastietojärjestelmän palvelimen tietoturvatapahtumia täytyy monitoroida säännöllisesti.” (Tietosuojavaltuutettu, 2021)

Tietosuojavaltuutetun Vastaamoa koskevasta päätöksestä ei suoraan voi yleistää, että Nixun esittämät turvallisen palvelun ylläpidon parhaat käytänteet muodostaisivat kaikissa tapauksissa asianmukaisten teknisten ja organisatoristen toimenpiteiden velvoittavuuden vähimmäistason. Kuitenkin päätöstä voi-

daan tulkita niin, että palomuurien hyödyntäminen, salasanapolitiikka, tietoliikenneyhteyksien salaaminen, lokitietojen hallinta, järjestelmien eriyttäminen, tietoturvapäivitysten ajantasaisuus ja tietoturvapoikkeamien valvonta ovat kaikki keskeisiä osa-alueita teknisistä ja organisatorisista toimenpiteistä.

Teknisten ja organisatoristen toimenpiteiden laajuutta voi lähestyä myös standardien ja standardointilaitosten kannanottojen kautta. Euroopan telealan standardointilaitos (European Telecommunications Standards Institute, ETSI) on yksi kolmesta EU:n tunnustamasta eurooppalaisesta standardointiorganisaatiosta. Organisaatio on julkaissut teknisiä selvennyksiä sisältävän raportin, jonka avulla teknisten ja organisatoristen riskienhallintakeinoja on mahdollista määritellä. Dokumenttia ei kuitenkaan nimenomaisesti ole tarkoitettu normatiivista sääntelyä varten. ETSI on määrittänyt kriittisille turvallisuustoimenpiteille 20 kohdan listan[12], joista erityisesti kuusi ensimmäistä ovat kaikkein keskeisimpiä ja tulisi toteuttaa aivan ensimmäisenä:

1. Käytetyn laitteiston listaaminen ja kontrollointi
2. Käytettyjen ohjelmistojen listaaminen ja kontrollointi
3. Jatkuva haavoittuvuuksien hallinta
4. Pääkäyttäjäoikeuksien kontrolloitu käyttö
5. Turvaa mobiilipäätelaitteiden, työasemien ja servereiden laitteiston ja ohjelmistojen konfiguraatiot
6. Lokitietojen ylläpito, valvonta ja analysointi. (ETSI, 2018, s. 5 ja 9)

ETSI 20 kohdan listassa kohdat 17-20 on erikseen nimetty organisatoriksi toimenpiteiksi, koska teknisten ratkaisujen sijaan nämä toimenpiteet kohdistuvat enemmän ihmisiin ja prosesseihin. Näistä ihmisiin ja prosesseihin keskittyvistä

---

[12] CSC 1: Inventory and Control of Hardware Assets
CSC 2: Inventory and Control of Software Assets
CSC 3: Continuous Vulnerability Management
CSC 4: Controlled Use of Administrative Privileges
CSC 5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7: Email and Web Browser Protections
CSC 8: Malware Defences
CSC 9: Limitation and Control of Network Ports, Protocols, and Services
CSC 10: Data Recovery Capabilities
CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12: Boundary Defence
CSC 13: Data Protection
CSC 14: Controlled Access Based on the Need to Know
CSC 15: Wireless Access Control
CSC 16: Account Monitoring and Control
CSC 17: Implement a Security Awareness and Training Program
CSC 18: Application Software Security
CSC 19: Incident Response and Management
CSC 20: Penetration Tests and Red Team Exercises

toimenpiteistä voidaan saada myös tulkinta-apua siihen, mitä direktiivissä organisatorisilla toimenpiteillä voitaisiin tarkoittaa:

> 17. Turvallisuustietoisuuden ja harjoittelun koulutusohjelman toteuttaminen
> 18. Sovellusten elämänkaarenhallinta
> 19. Poikkeamien hallinnan ja niihin vastaaminen
> 20. Turvallisuustestaukset (penetraatiotestaus) ja hyökkäysten torjunnan (red team) harjoittelu. (ETSI, 2018, s. 5 ja 9)

ETSI organisaatio lisäksi useita muita standardeihin perustuvia vaihtoehtoja teknisten ja organisatoristen keinojen vähimmäistason tulkitsemiseksi löytyy siinä määrin, että standardien ja mittaristojen runsaus voidaan nähdä myös ongelmana. NIS-direktiivin toimeenpanoon liittyviä parhaita käytäntöjä EU-tasolla käsittelevä koordinaatioryhmä joutui toteamaan raportissaan, että jäsenvaltiot haluavat käyttää erilaisia tietoturvallisuuden hallinnan mittaristoja ja vaatimusten tarkkuuden taso tämän takia vaihtelee jäsenmaittain. Koordinaatioryhmä on julkaissut 27 kohtaisen listan tietoturvan osa-aluista, jotka suositellaan ainakin huomioitavan. (NIS CG, 2018a, s. 7) Mittaristoihin ja standardeihin liittyen EU:n kyberturvallisuusvirasto ENISA suosittaa riskienhallinnan toteuttamiseksi ISO 27000 standardisarjan noudattamista, minkä lisäksi markkinaehtoisten toimijoiden suositetaan osoittavan heidän tietoverkkojen turvallisuuden hyödyntämällä Common Criteria (suositus) tai vastaavaa viitekehystä kuten ISO 15408 ja NIST SP 800. ENISA:n suosituksessa on erityisen huomionarvoista, että pitäisi kuitenkin täsmällisemmin määrittää, mikä turvallisuustaso tietyllä mittarilla tulisi saavuttaa. (ENISA, 2016, s. 20) Vaikuttaisi siltä, että mikäli tietyn standardisarjan kautta teknisten ja organisatoristen toimenpiteiden vähimmäistasoa haluttaisiin määrittää, ISO 27000 sarja voisi tarjota tähän hyvän lähtökohdan. Suomessa Valtioneuvoston periaatepäätöksessä tietoturvan ja tietosuojan parantamisesta yhteiskunnan kriittisillä toimialoilla (TITUKRI) linjataan, että NIS-direktiivissä määritellyillä toimialoilla tulee huolehtia, että "kriittisten toimialojen suurimpien ja yhteiskunnan keskeisten toimintojen kannalta merkittävimpien toimijoiden tulee osoittaa käyttävänsä tietoturvallisuuden hallintajärjestelmää ISO 27001 –sertifioinnilla tai sitä vastaavalla yleiseen tietoturvastandardiin perustuvalla sertifioinnilla vuoden 2025 loppuun mennessä". (Valtioneuvosto, 2021, s. 8) Periaatepäätöksen toimeenpano vaikuttaisi kuitenkin ainakin osittain olevan sidoksissa sen toteuttamiseksi mahdollisesti myönnettävään lisärahoitukseen.

Edellä esitetyn perusteella voidaan yhteenvetona todeta, että yhteiskunnan keskeisen palvelun tarjoaja on velvollinen hallitsemaan viestintäverkkoihin ja tietojärjestelmiin kohdistuvia riskejä. Riskienhallinnan tulisi olla asianmukaista ja oikeasuhtaista, mutta asianmukaisuuden ja oikeasuhtaisuuden arvioinnille ei ole määritetty mittatikkua, jota vasten voitaisiin määrittää jonkinlainen vähimmäistaso. Toimijan suojaksi on myös säädetty eräänlainen asianmukaisuuden ja oikeasuhtaisuuden yläraja eli toimijalta ei saisi velvoittaa tietyn teknologisen ratkaisun käyttämistä vaan toimijalla tulisi olla vapaus valita keinot, kuinka haluttu tavoitetila saavutetaan. Riskienhallintavelvollisuus kattaa sekä tekniset että or-

ganisatoriset toimenpiteet, jotka koostuisivat vähintään poikkeamien riskin tunnistamisesta, poikkeamien estämisestä, havaitsemista, käsittelemistä ja poikkeamien vaikutusten lieventämisestä. Siinä missä tietyn teknologisen ratkaisun käyttämistä ei vaadita niin myöskään tietyn standardin tai mittariston käyttöä ei suoraan vaadita. Kuitenkin sekä ENISA:n että Valtioneuvoston periaatepäätöksen kautta on mahdollista suosittaa ISO 27000 standardisarjaa ja erityisesti ISO 27001 standardia teknisten ja organisatoristen toimenpiteiden tavoitetasoksi.

2.2.1.2 Kyky suojautua tietyllä varmuudella tietoja tai palvelun saatavuutta vaarantavilta toimilta.

Hallituksen esityksen mukaan riskienhallinnan tarkoituksena on varmistaa ”viestintäverkkojen ja tietojärjestelmien kyky suojautua tietyllä varmuudella toimilta, jotka vaarantavat tallennettujen tai siirrettyjen tai käsiteltyjen tietojen taikka muiden kyseisissä järjestelmissä tarjottujen tai niiden välityksellä saatavilla olevien palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden.” (HE 192/2017 vp, s. 70, 71, 73, 76 ja HE 34/2018 vp, s. 66) Hallituksen esityksen teksti vastaa tältä osin NIS-direktiivin 4(1) artiklan määritelmää verkkoja tietojärjestelmien turvallisuudesta. Edellä käsiteltyjen asianmukaisten teknisten ja organisatoristen riskienhallintakeinojen tarkoitus olisi siis varmistaa kykyä suojautua tietyllä varmuudella, mutta mitä tietyllä varmuudella tarkoitetaan? Direktiivin 14(1) artiklan mukaan asianmukaisten ja oikeasuhtaisten teknisten ja organisatoristen riskienhallintakeinojen tarkoitus on varmistaa riskiin suhteutettu verkko- ja tietojärjestelmien turvallisuuden taso uusin tekniikka huomioiden. Kyky suojautua tietyllä varmuudella voitaisiin siis nähdä tarkoittavan samaa kuin riskiin suhteutettu tai riskiperustaisuus. Tulkinta saa myös tukea Ruotsin vastaavasta säädöksestä, jossa toimijoiden velvollisuutena on tehdä systemaattista ja riskiperustaista (systematiskt och riskbaserat) tietoturvatyötä. (Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, 11 §)

Edellä mainitun ETSI organisaation raportin mukaan riskiperustaisuudella tarkoitetaan, että käytetyt turvajärjestelmät perustuvat riskeihin ja ovat priorisoituja mahdollistaen organisaation turvallisuuteen kohdistuvien investointipäätösten pohjautumisen riskien tilannekuvaan ja tunnustaen, että millään organisaatiolla ei ole rajattomia resursseja. Riskiperustaiset turvallisuuskäytännöt pystyvät heijastamaan organisaation liiketoiminnallisia ajureita ja turvallisuushakuisuutta. (ETSI, 2018, s. 18)

Riskiperustaisen lähestymistavan keskiössä on riskien tunnistaminen, koska ilman riskien tunnistamista on vaikea arvioida, tuottavatko turvallisuustoimenpiteet riittävän varmuuden suojautumiskyvystä. Tämän takia toimijan tulisi laatia riskianalyysi. Vertailun vuoksi NIS-direktiivin toimeenpanoa tukeva koordinaatioryhmä suosittaa riskianalyysin laatimista ja sen säännöllistä päivittämistä. (NIS CG, 2018a, s. 14) Ruotsin lainsäädännössä velvollisuus tehdä riskianalyysi on kirjattu lakiin. (Lag (2018:1174) 14 §) Jäljempänä dokumentointivelvollisuutta koskevassa alakappaleessa käsittelen mitä dokumentaatiota toimijalta vaaditaan. Suomen kansallinen lainsäädäntö ei tällä hetkellä ehdottomasti

vaadi riskianalyysin dokumentointia, mutta riskienhallinnan dokumentaation uskottavuutta voi olla vaikea todistaa, mikäli riskianalyysiä ei ole dokumentoitu.

Vertailun vuoksi kuitenkin laki julkisen hallinnon tiedonhallinnasta 13.1 § velvoittaa viranomaisten tiedonhallintayksiköitä selvittämään olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoittamaan tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Julkisen hallinnon tiedonhallintalakia koskevan hallituksen esityksen yksityiskohtaisten perusteluiden mukaan pykälä

> ”[m]uodostaisi kokonaisuuden, johon kuuluisi riskien arviointi, tietoturvallisuustoimenpiteiden suunnittelu tunnistettujen riskien perusteella sekä tietoturvallisuustoimenpiteiden toteuttaminen. Riskienarviointi ei olisi kertaluonteista, vaan jatkuvaa toimintaa, jossa muun muassa arvioidaan suunnitelmien toteutumista ja toteutettujen tietoturvatoimenpiteiden vaikuttavuutta.” (HE 284/2018 vp, s. 92)

Yhteenvetona kappaleesta voidaan todeta, että kansallisessa sääntelyssä esiintyvä käsite kyky suojautua tietyllä varmuudella tietoja tai palvelun saatavuutta vaarantavilta toimilta voidaan tulkita tarkoittavan samaa kuin direktiivissä käytetty ilmaus riskiin suhteutettu tai Ruotsin lainsäädännössä käytetty ilmaus riskiperustainen. Keskeisenä edellytyksenä tietyn varmuuden tai riskiperustaisuuden määrittämiselle on riskianalyysin laatiminen turvallisuustoimenpiteiden mitoittamiseksi.

2.2.1.3 Riski

Hallituksen esityksen yksityiskohtaisten perusteluiden mukaan riskillä tarkoitettaisiin mitä tahansa kohtuullisesti tunnistettavissa olevaa tilannetta tai tapahtumaa, joka saattaa vaikuttaa haitallisesti viestintäverkkojen ja tietojärjestelmien turvallisuuteen. (HE 192/2017 vp, s. 70, 71, 73, 76 ja HE 34/2018 vp, s. 66) Hallituksen esityksen määritelmä vastaa NIS-direktiivin 4 artiklan 9 kohdan määritelmää. Riskin määritelmästä ensimmäisenä voidaan havaita, että tarkastelukulma ei rajaudu tekniseen tietoturvallisuuteen kuten tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuuteen vaan edellyttää kaikkien uhkatekijöiden huomioimista, olivat ne sitten luonnon tai ihmisen aiheuttamia, onnettomuuksia tai tahallaan aiheutettuja (ns. all-hazard approach).[13] Tällöin esimerkiksi Katarkri2020 käsitteillä ilmaistuna riskejä tunnistettaessa tulisi huomioida niin turvallisuusjohtaminen, fyysinen turvallisuus kuin tekninen tietoturvallisuuskin. (Katakri, 2020, s. 8) Katakri2020 mukaan:

> ”Tietoturvallisuusriskien hallintaprosessi koostuu toimintaympäristön määrittämisestä, riskien arvioinnista (tunnistaminen, analysointi, merkityksen arviointi), riskien

[13] Ehdotuksessa Euroopan parlamentin ja neuvoston direktiiviksi kriittisten toimijoiden häiriönsietokyvystä (16.12.2020) johdantotekstin kohdassa 7 esitetään määritelmä kaikkien uhkatekijöiden huomioimiseksi (ns. all-hazard approach): Tällä direktiivillä luodaan yhtenäinen kehys kriittisten toimijoiden häiriönsietokyvyn vahvistamiseksi kaikkia uhkatekijöitä vastaan, olivat ne sitten luonnon tai ihmisen aiheuttamia, onnettomuuksia tai tahallaan aiheutettuja.

käsittelystä, riskien hyväksynnästä, riskejä koskevasta viestinnästä ja tiedonvaihdosta sekä riskien seurannasta ja katselmoinnista." (Katakri, 2020, s. 11)

Kaikkien uhkatekijöiden tunnistamiseksi toimijalta ei kuitenkaan vaadita rajattomia kykyjä vaan riittävää on kohtuullisesti tunnistettavissa olevien tilanteiden ja tapahtumien huomiointi. Kohtuullisesti tunnistettavissa käsitettä ei ole mahdollista yksiselitteisesti määritellä, mutta käsitteestä voidaan todeta se, että sen merkitys elää ajassa. Yksi kansallisten toimivaltaisten viranomaisten, kyberturvallisuuskeskusten, EU:n kyberturvallisuusvirasto ENISA:n ja NIS koordinaatioryhmän tehtävistä on jakaa tietoa riskeistä ja tapahtuneista tietoturvapoikkeamista. Lisäksi NIS-direktiivin yksi keskeinen toiminto on merkittävistä poikkeamista ilmoittaminen. Merkittävistä poikkeamista ilmoittamisen yksi tarkoitus on mahdollistaa ennakkovaroituksen antaminen muille toimijoille uhkasta, jolloin muut toimijat voivat huomioida kyseisen riskin. Tiedon jakaminen toteutuneista poikkeamista sekä riskeistä merkitsee sitä, että aikaisemmin raportoitua poikkeamaa tai tunnistettua riskiä tulisi jatkossa aina pitää kohtuullisesti tunnistettavissa olevana.

2.2.1.4 Dokumentaatiovelvollisuus

Hallituksen esityksen yksityiskohtaisten perusteluiden mukaan riskienhallinnan dokumentoinnin tulisi olla todennettavassa muodossa. (HE 192/2017 vp, s. 70, 71, 73, 76 ja HE 34/2018 vp, s. 66) NIS-direktiivin artikla 15 velvoittaa jäsenvaltioita varmistamaan, että toimivaltaisilla viranomaisilla on valtuudet pyytää keskeisen palvelun tarjoajalta todennettavassa muodossa olevat turvallisuusohjeet (en. *documented security policies*, sv. dokumenterade säkerhetsprinciper). Suomessa dokumentaatiovelvollisuus ei ole sidottu esitysmuotoon, mutta kirjallisista muodoista esimerkiksi Intranet-sivu tai toiminnanohjausjärjestelmän työmääräys (tiketti) edustavat hyviä käytäntöjä. (Katakri, 2020, s. 8) Dokumentaatiovelvollisuuden osalta ajan kulumisen huomioimista ei ole kansallisella eikä EU-tasolla säännelty eli sääntely ei ota kantaa esimerkiksi siihen, tulisiko vain tuoreimmat versiot dokumenteista olla olemassa vai tulisiko esimerkiksi aikaisempia riskiarvioita tai vastaavia myös säilyttää. Huomionarvoista on, että siinä missä direktiivin eri kieliversioissa käsitellään turvallisuusohjeita, turvallisuuspolitiikkoja tai turvallisuusperiaatteita, Suomessa dokumentaatiovelvollisuus vaikuttaisi koskevan riskienhallintaa laajemmin. Katakri2020 näkökulmasta riskienhallinnan laajempi dokumentointi on suotavaa, koska "[h]yvään turvallisuusjohtamiseen kuuluu menettelytapojen ja erityisesti riskien arvioinnin dokumentointi." (Katakri, 2020, s. 8) Dokumentointivelvollisuuden yksi erinomainen piirre on, että dokumentointivelvollisuus voi ohjata hyväksymään asiakirjat toimijan organisaatiorakenteen mukaisesti ylemmässä johdossa, mikä toivottavasti edelleen lisää ylemmän johdon sitoutuneisuutta ja tukea riskienhallinnan toteuttamiseen. Riskienhallinnan dokumentaatiovelvollisuuden sisällön laajentaminen direktiivin sanamuodosta on selkeä poliittinen valinta, mutta ei EU-alueella ainutlaatuista. Esimerkiksi Ruotsissa yhteiskunnan keskeisten toimijoiden on tehtävä turvallisuustoimenpidesuunnitelma, jonka pohjana on riskianalyysi, joka on

dokumentoitava ja päivitettävä vuosittain. (Lag (2018:1174) 12 §) Vaikka dokumentaatiovelvollisuus on Suomessa NIS-direktiivin vähimmäistasoa aavistuksen laajempi niin sen voi kuitenkin katsoa olevan suppeampi kuin esimerkiksi tietosuoja-asetuksen osoitusvelvollisuus. Tietosuoja-asetuksen 5(2) artiklassa käytetään käsitettä osoitusvelvollisuus kuvaamaan rekisterinpitäjän velvollisuutta pystyä tarvittaessa osoittamaan, että se on noudattanut henkilötietojen käsittelyä koskevia vaatimuksia. NIS-direktiivin dokumentaatiovelvollisuuden laajuutta ei voi pitää yhtä kattavana kuin tietosuoja-asetuksen osoitusvelvollisuutta, koska niiden tarkoitukset ovat erilaiset. Tietosuoja-asetuksen osoitusvelvollisuuden tarkoituksena on osoittaa ulkopuolisille, että asetuksen velvollisuuksia noudatetaan. NIS-direktiivin mukaan dokumentaatiovelvollisuuden ensisijainen tarkoitus on edistää toimijan tietoista riskienhallintaa ja riskienhallintakeinojen oikeasuhtaista mitoittamista. (HE 192/2017 vp. s. 70, 71, 73, 76 sekä HE 34/2018 vp. s. 66)

Yhteenvetona riskienhallintavelvollisuuteen sisältyvän dokumentaatiovelvollisuudesta voidaan todeta, että dokumentaatio tulee olla todennettavassa muodossa ja vähimmäistason täyttämiseen ei riitä turvallisuusohjeen ja turvallisuuspolitiikan kirjallinen dokumentointi vaan velvollisuus on laajempi. Kuitenkaan laajuuden vähimmäistasosta ei voi tehdä tarkempia johtopäätöksiä, vaan laajuus tulee suhteuttaa yhteiskunnan keskeisen palvelun merkittävyyteen ja hyväksyttävän jäännösriskin suuruuteen pitäen mielessä, että dokumentaation ensisijainen tarkoitus on edistää toimijan tietoista riskienhallintaa ja riskienhallintakeinojen oikeasuhtaista mitoittamista. Luonnollisesti dokumentaatio helpottaa sääntelyn noudattamisen valvontaa, mutta yksinomaan velvollisuuksien noudattamisen valvontaa palvelevaa dokumentaatiota ei ole tarkoituksenmukaista vaatia tehtävän.

2.2.1.5 Uusin tekniikka huomioiden

NIS-direktiivin perusteella annetussa kansallisessa sääntelyssä uusimman tekniikan käsitettä ei ole käytetty. NIS-direktiivin 14(1) artiklan mukaan riskiin suhteutettu verkko- ja tietojärjestelmien turvallisuuden taso on varmistettava uusin tekniikka huomioon ottaen. Direktiivin johdantotekstin kohdassa 52 lisäksi todetaan, että riskienhallintavaatimusten tulee oikeassa suhteessa kulloisenkin verkko- ja tietojärjestelmän aiheuttamaan riskiin ottaen huomioon tällaisiin toimenpiteisiin käytettävä uusin tekniikka. Käsite uusin tekniikka huomioiden (en. state of the art, sv. den senaste tekniska utvecklingen) kattaa tässä yhteydessä selkeästi uusimmat tekniset riskienhallintakeinot, mutta käsite tulisi ymmärtää kattavan myös edistyksen kaikissa muissakin kuin puhtaasti teknisissä riskienhallintakeinoissa, esimerkiksi organisatoriset riskienhallintakeinot ja inhimilliset tekijät niiden osana. Lisäksi uusimman tekniikan huomiointi riskienhallinnassa tulisi ymmärtää käsittävän myös tietoturvauhkiin liittyvän uusiman tekniikan huomioimisen. Tietoturvauhkiin liittyvää uusinta tekniikkaa ei voine tyhjentävästi määritellä, mutta sen tulisi esimerkiksi kattaa hyökkäysvektoreiden kehittymisen, uusien raportoitujen haavoittuvuuksien hallinnan, mahdollisten hyökkääjien toimintatapojen ymmärtämisen (taktiikat, tekniikat ja menetelmät) sekä ylipäänsä uhkien tilannekuvan (threat landscape) muutosten ymmärtämisen.

Uusimman tekniikan käsite merkitsee myös ajallisen ulottuvuuden huomioimista. Riskienhallinta on jatkuva prosessi, joka tulee huomioida viestintäverkkojen ja tietojärjestelmien koko elinkaaren aikana. Otettaessa uusia suojaustoimenpiteitä tänään käyttöön, ne toivottavasti käyttöönottohetkellä edustavat riskienhallinnan näkökulmasta uusinta tekniikka. Kuitenkin käyttöönoton jälkeinen ajan kuluminen voi merkitä, että käyttöönottohetken riskienhallintamenetelmät eivät enää täytä direktiivin vähimmäisvaatimusta vaan ajan kuluessa riskienhallintamenetelmiä on kehitettävä. Käytännössä uuteen tekniikkaan liittyvän ajallisen näkökulman huomiointi vaatii tunnistamaan, milloin tietyt olemassa olevat turvallisuustoimenpiteet ovat muuttuneet tehottomiksi.

EU-oikeudessa uusimman tekniikan käsitettä hyödynnetään useilla eri oikeudenaloilla. EU:n tietotekniikkaa koskevan sääntelyn osalta mahdollisesti varhaisin esimerkki on jo vuonna 2009 jäsenvaltiolle kohdistettu velvoite edellytettiin huomiovan uusin tekniikka sähköisten viestintäpalveluiden tarjoajien tietoturvavaatimuksissa (EU direktiivi 2009/140/EY artikla 13 a). Lisäksi NIS-direktiivin kanssa samanaikaisesti valmistellut tietosuoja-asetuksen 32 artiklan mukaan uusin tekniikka tulee huomioida teknisten ja organisatoristen turvallisuustoimenpiteiden asianmukaisuutta arvioitaessa.

Yhteenvetona voidaan todeta, että Suomessa verkko- ja tietojärjestelmien turvallisuussääntelyn riskienhallintavelvoite vaikuttaisi olevan NIS-direktiivin sanamuodon vähimmäistasoa alempi siltä osin, kun uusinta tekniikkaa ei suoranaisesti vaadita huomioitavan. Uusimman tekniikan voi ymmärtää sisältävän niin uusimpien teknisten kuin myös organisatoristen riskienhallintakeinojen hyödyntämisen, minkä lisäksi sen tulisi ymmärtää kattavan myös tieturvauhkiin liittyvän uusimman tekniikan eli hyökkäyksellisen näkökulman huomioimisen. Lisäksi uusin tekniikka tulisi ymmärtää kattavan myös ajan kulumiseen liittyvän näkökulman. Uusimman tekniikan käsite esiintyy myös muualla EU-oikeudessa, mikä mahdollistaa myös tulkinnan, että kyseessä on yleisempi EU-oikeudellinen periaate ja siten periaatteena uusin tekniikka voitaisiin huomioida osana riskienhallinnan asianmukaisuuden kokonaisuutta ilman suoraa lakiin kirjoitettua velvoitetta. Vaikuttaisi myös siltä, että riskienhallintavelvollisuuden kokonaisuudesta ei pystytä oikeudellisesti ennakolta määrittämään, mikä on riittävä riskienhallinnan taso. Tämä merkitsee, että toistaiseksi vähimmäistaso muotoutuu valvovan viranomaisen jälkikäteisten tulkintakannanottojen kautta. Kun riskienhallintavaatimuksen sisältöä ei pystytä tutkielmassa käytettyjen oikeuslähteiden perusteella määrittämään, ongelmaa voisi olla hyvä lähestyä jollakin toisella tutkimusmetodilla. Vaihtoehtoisesti riskienhallintavelvollisuuden tasoa voitaisiin pyrkiä määrittelemään organisaatioiden itsensä näkökulmasta esimerkiksi systeemiajattelua hyödyntäen, josta esimerkkinä on Pöyhösen väitöskirja ”Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa”. (Pöyhönen, 2020).

2.2.2 Ilmoittamisvelvollisuus

Tässä kappaleessa selvitetään, minkälainen lakiin perustuva velvollisuus toimijoilla on ilmoittaa merkittävistä tietoturvapoikkeamista. Toisin sanoen kappaleessa vastataan kysymykseen, mistä tietoturvapoikkeamista toimijoiden tulee ilmoittaa. Tähän kysymykseen vastauksen antaminen edellyttää selvitettävän, että mitä laissa tarkoitetaan merkittävällä tietoturvapoikkeamalla.

Hallituksen esityksen mukaan tietoturvapoikkeamien ilmoittamisen yhteiskunnallisena hyötynä on, että valvovien viranomaisten tilannekuva paranee ja eri toimialojen tietoturvaosaaminen kasvaa. (HE 192/2017 vp, s. 61) Tietoturvaloukkauksista ilmoittaminen ei ole Suomen lainsäädännössä uusi ilmiö, vaan hieman laajempi ilmoitusvelvollisuus on säädetty teleyrityksille jo aikaisemmin (Laki sähköisen viestinnän palveluista 275.1 §). Vastaavasti tietoturvaloukkauksiin läheisesti liittyvistä henkilötietojen tietoturvaloukkauksista on tietosuoja-asetuksen 33 artiklan mukaisesti ilmoitettava ilman aiheetonta viivytystä. NIS-direktiivin mukainen tietoturvapoikkeaminen ilmoittamisvelvollisuus on kirjattu liikenteen toimijoiden osalta sektorikohtaiseen lainsäädäntöön samalla tavoin kuin myös riskienhallintavelvoite. Ilmoittamisvelvollisuutta koskevat lakipykälät sekä lakien esitöistä hallitusten esitysten yksityiskohtaiset perustelut olennaisilta osin on kerätty alla olevaan taulukkoon. Taulukossa on alleviivattu ne kohdat, jotka sanamuodoltaan selkeästi poikkeavat muista kohdista.

TAULUKKO 2 Velvoitteet häiriöistä ilmoittamiseksi

Toimija	Laki	Hallituksen esityksen tarkenne	Hallituksen esityksen vähimmäistaso
Tieliikenteen ohjaus- ja hallintapalvelun tarjoajan	on ilmoitettava viipymättä Liikenne- ja viestintävirastolle sellaisesta sen järjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, joka voi aiheuttaa merkittävän vaaran liikenteen turvallisuudelle. (Laki liikenteen palveluista 140.2 §)	Tietoturvallisuuteen liittyvällä häiriöllä tarkoitettaisiin mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti kyseessä olevien järjestelmien turvallisuuteen. (HE 34/2018 vp, s. 86)	Merkittävänä olisi pidettävä häiriötä, joka voisi aiheuttaa liikenneturvallisuudelle riskin. Poikkeaman merkittävyyden määrittämiseksi olisi otettava huomioon erityisesti niiden käyttäjien lukumäärä, joihin häiriö vaikuttaa, poikkeaman häiriön kesto sekä maantieteellinen levinneisyys. (HE 34/2018 vp, s. 86)
Älykkään liikennejärjestelmän ylläpitäjän	on ilmoitettava viipymättä Liikenne- ja viestintävirastolle sen käyttämiin viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä. (Laki liikenteen palveluista 161.2 §)	Tietoturvallisuuteen liittyvällä häiriöllä tarkoitettaisiin mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti kyseessä olevien järjestelmien turvallisuuteen. (HE 192/2017 vp, s. 76)	Merkittävänä olisi pidettävä häiriötä, joka voi muodostaa älykkään liikennejärjestelmän turvallisuudelle merkittävän riskin. Poikkeaman merkittävyyden määrittämiseksi olisi otettava huomioon erityisesti niiden käyttäjien lukumäärä, joihin häiriö vaikuttaa, häiriön kesto sekä maantieteellinen levinneisyys. (HE 192/2017 vp, s. 76)
Valtion rataverkon haltijan sekä liikenteenohjauspalvelun tarjoajan	on ilmoitettava viipymättä Liikenne- ja viestintävirastolle viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä. (Raideliikennelaki 169.2 §)	Tietoturvallisuuteen liittyvällä häiriöllä tarkoitettaisiin mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti kyseessä olevien järjestelmien turvallisuuteen. (HE 192/2017 vp, s. 70)	Merkittävänä olisi pidettävä häiriötä, joka voisi aiheuttaa rautatiejärjestelmälle vastaavan merkittävän turvallisuusriskin kuin on tarkoitettu rautatielain 39 §:n 2 momentissa. Poikkeaman merkittävyyden määrittämiseksi olisi otettava huomioon erityisesti niiden käyttäjien lukumäärä, joihin häiriö vaikuttaa, häiriön kesto sekä maantieteellinen levinneisyys. (HE 192/2017 vp, s. 70)
VTS-palveluntarjoajan	on ilmoitettava viipymättä Liikenne- ja viestintävirastolle käyttämiinsä viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä. (Alusliikennepalvelulaki 18 a.1 §)	Tietoturvallisuuteen liittyvällä häiriöllä tarkoitettaisiin mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti kyseessä olevien järjestelmien turvallisuuteen. (HE 192/2017 vp, s. 72)	Merkittävänä olisi pidettävä häiriötä, joka voisi merkittävästi vaikuttaa merenkulun turvallisuuteen. Häiriön merkittävyyden määrittämiseksi olisi otettava huomioon erityisesti niiden käyttäjien lukumäärä, joihin häiriö vaikuttaa, häiriön kesto sekä maantieteellinen levinneisyys. (HE 192/2017 vp, s. 72)
Yhteiskunnan toiminnan kannalta merkittävän satamanpitäjä	on ilmoitettava viipymättä Liikenne- ja viestintävirastolle sen käyttämiin viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä. (Turvatoimilaki 7 f.1 §)	Tietoturvallisuuteen liittyvällä häiriöllä tarkoitettaisiin mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti kyseessä olevien järjestelmien turvallisuuteen. (HE 192/2017 vp, s. 74)	Merkittävänä olisi pidettävä häiriötä, joka voisi merkittävästi vaikuttaa merenkulun turvallisuuteen. Poikkeaman merkittävyyden määrittämiseksi olisi otettava huomioon erityisesti niiden käyttäjien lukumäärä, joihin häiriö vaikuttaa, poikkeaman kesto sekä maantieteellinen levinneisyys. (HE 192/2017 vp, s. 74-75)

Yleisesti luonnehtien tietoturvallisuuteen liittyvistä häiriöistä ilmoittamisvelvoite on kaikille liikennejärjestelmän toimijoille pykälätasolla sama ja hallituksen esityksessä korostetaan, että määritelmä vastaa NIS-direktiivin määritelmää. Lakiin perustuva ilmoitusvelvollisuus sanamuodon mukaisesti koskee kyseistä toimijaa, vaikka tietoturvallisuuteen liittyviä toimintoja olisi ulkoistettu tai siirretty toisen viranomaisen hoidettavaksi.

Ilmoitus on tehtävä viipymättä eli 14(3) artiklan sanamuodon mukaisesti ilman aiheetonta viivytystä. NIS-koordinaatioryhmän mukaan ilman aiheetonta viivytystä olisi esimerkiksi ilmoittaminen heti kun toimija itse on merkittävästä poikkeamasta tietoinen tai heti kun muutoksen aiheuttava poikkeama tapahtuu. (NIS CG, 2018b, s. 9) Vertailun vuoksi tietosuoja-asetuksen kohdalla poikkeamasta tietoisuudella tarkoitettaisiin kohtuullista todennäköisyyttä (”a reasonable degree of certainty”) siitä, että turvallisuuspoikkeama on tapahtunut.

Poikkeamasta tietoisuuden käsite voisi tällöin sisältää lyhyen hetken henkilötietojen tietoturvapoikkeaman olemassaolon tai tapahtumisen todentamiselle, jolloin tietoturvapoikkeamasta tietoisuuden kynnyksen ei vielä katsottaisi ylittyneen. (Tietosuojatyöryhmä WP 29, 2018, s. 11)

Ilmoitusvelvollisuuden osalta laissa ei aseteta tarkempia vaatimuksia sille, minkälainen ilmoituksen tulisi olla. NIS-koordinaatioryhmä on tuonut esille, että useissa jäsenvaltioissa on käytössä kaksi tai kolmivaiheinen ilmoittaminen. Tällöin ensi-ilmoituksen tarkoitus olisi viranomaisen huomion herättäminen ja ilmoitus voisi sisältää oletuksia ja ennusteita vaikutuksista. Mahdollinen väliraportti laadittaisiin, kun uutta tietoa on saatavilla ja loppuraportti laadittaisiin häiriön käsittelyn päätyttyä. (NIS CG, 2018b, s. 9)

Pykälien sanamuodossa on hienoisia muotoilueroja mihin järjestelmiin liittyvistä häiriöistä tulee ilmoittaa, mutta säädösten systematiikan kannalta on selvää, että ilmoittamisvelvoite koskee niitä viestintäverkkoja ja tietojärjestelmiä, jotka ovat myös riskienhallinnan kohteena. Tieliikenteen ohjaus- ja hallintapalvelun tarjoajan kohdalla ilmoittamisvelvollisuutta on pykälätasolla rajattu koskemaan vain sellaisia häiriöitä, jotka voivat aiheuttaa merkittävän vaaran liikenneturvallisuudelle.

Tietoturvallisuuteen liittyvän häiriön määritelmä on kaikille liikennejärjestelmän toimijoille sama. Häiriöllä tarkoitettaisiin ”mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti kyseessä olevien järjestelmien turvallisuuteen”. Määritelmässä käytetty ilmaus ”mitä tahansa tapahtumaa” on loogisesti yhteydessä riskienhallintavelvollisuuden laajuuteen, jossa kaikki tekijät tulee huomioida (ns. all-hazard approach). Toiseksi määritelmästä on syytä korostaa tosiasiallista vaikutusta eli oletettu, teoreettinen tai mahdollinen vaikutus ei ylitä ilmoituskynnystä. Vastaavasti ETSI organisaatio esittää, että yritysasteelle jääneistä tietomurroista ei olisi tarvetta ilmoittaa. (ETSI, 2017, s. 14). Kolmanneksi häiriön määritelmässä on huomionarvioista, että se rajautuu kyseessä oleviin järjestelmiin eli vain niihin viestintäverkkoihin ja tietojärjestelmiin, jotka tunnistettiin edellä riskienhallintakappaleessa.

Edellä taulukko 2 esitetyn perusteella voidaan luokitella, että hallituksen esityksen mukaan häiriötä voitaisiin pitää merkittävänä kahden eri harkintakokonaisuuden perusteella. Näistä harkintakokonaisuuksista tutkielmassa käytetään käsitteitä turvallisuus ja jatkuvuus.

Ensimmäinen harkintakokonaisuus olisi turvallisuus. Tieliikenteenohjauksessa vaatimuksena on, että liikenneturvallisuudelle voisi aiheutua riski, VTS-palveluissa ja satamissa merenkulun turvallisuus voisi vaarantua, älykkäiden liikennejärjestelmien turvallisuudelle voisi muodostua merkittävä riski tai raideliikenteelle voisi aiheutua merkittävä riski[14]. Edellä mainituista turvallisuusris-

[14] Rautatiejärjestelmän osalta viittaus rautatielain 39.2 §:ään on epäselvä, koska jo kumotussa rautatielain 39.2 §:ssä ei määritellä merkittävää turvallisuusriskiä. Kuitenkin kyseisen py-

keistä on syytä huomata, että älykkäiden liikennejärjestelmien kohdalla turvallisuusriskin kohteena olisi järjestelmä itsessään, esimerkiksi liikennejärjestelmien keskeisiä palveluita koskevassa kappaleessa mainittu eCall -hätäpuhelujärjestelmä. eCall -hätäpuhelujärjestelmän osalta tämä on myös hyvin looginen tulkinta, koska hätäpuhelu lähtökohtaisesti aktivoituu vasta liikenneturvallisuuden vaarannuttua eli onnettomuuden jo tapahduttua, jolloin järjestelmä itsessään harvoin voisi olla juurisyy liikenneturvallisuuden vaarantumiselle.

Toinen poikkeaman merkittävyyden harkintakokonaisuus olisi jatkuvuus. Poikkeaman merkittävyyden määrittämisessä taulukossa 2 viitattujen hallituksen esitysten mukaan olisi huomioitava häiriön vaikutuspiirissä olevien käyttäjien määrä, poikkeaman kesto ja maantieteellinen levinneisyys. Huomionarvoista käyttäjien lukumäärän, ajallisen keston ja maantieteellisen levinneisyyden harkintakriteerissä on, että tässä yhteydessä on mahdollista arvioida liikennejärjestelmää kokonaisuutena. Esimerkiksi satamien tilanteessa häiriön vaikutuspiirissä voisivat olla sekä merenkulun logistiikkaan, sataman raideliikenteeseen, että sataman maantiekuljetuksiin liittyvät käyttäjät.

Kriteerit käyttäjät, aika ja maantiede perustuvat NIS-direktiivin 14(4) artiklaan ja niiden soveltamisen taustalla on direktiivin määritelmä poikkeamien ilmoituskynnyksestä, joka määritellään merkittäväksi vaikutukseksi niiden tarjoaman palvelun jatkuvuuteen. NIS-direktiivin johdantokappaleissa 27 ja 28 tarkennetaan merkittävän haitallisen vaikutuksen määrittelyyn liittyviä tekijöitä. Johdantokappale 27 mukaan:

> ”Jäsenvaltioiden olisi otettava huomioon useita eri tekijöitä, kuten niiden käyttäjien lukumäärä, jotka ovat riippuvaisia kyseisestä palvelusta henkilökohtaisten tai ammatillisten tarkoitusten vuoksi. Kyseisen palvelun käyttö voi olla suoraa, epäsuoraa tai välityksen kautta tapahtuvaa. Arvioidessaan vaikutusta, joka poikkeamalla voisi vakavuutensa ja kestonsa perusteella olla talouden ja yhteiskunnan toimintoihin tai yleiseen turvallisuuteen, jäsenvaltioiden olisi arvioitava myös aika, joka todennäköisesti kuluu, ennen kuin palvelun keskeytymisellä alkaisi olla kielteinen vaikutus.”

Lisäksi johdantokappale 28 mukaan toimialakohtaiset tekijät kuten haitallisten vaikutuksen kohdentumisen osuus suhteessa kansalliseen liikennemäärään tai rahtikuljetusten lukumäärään vuodessa voitaisiin huomioida.

NIS-direktiivin koordinaatioryhmän mukaan käyttäjien määrän, ajan ja maantieteen lisäksi yhteiskunnan keskeisten palveluiden tarjoajien määrittämisessä käytettyä listaa (NIS-direktiivin 6 artikla) voi soveltaa myös poikkeaman merkittävyyden arviontiin. (NIS CG, 2018b, s. 8) Kyseisiä kriteereitä on käsitelty tässä tutkimuksessa edellä kappaleessa 2.1 liikennejärjestelmän keskeiset palvelut. Koordinaatioryhmä myös esittää, että NIS-direktiivin yhteydessä käsite jatkuvuus ymmärrettäisiin palvelun tarjoamisena sovitun tai kohtuullisen laatuta-

---

kälän esitöissä todetaan tarkoituksena olleen rautatiejärjestelmän korkean turvallisuustason säilyttäminen ja kehittäminen ”unionilainsäädännön ja alan teknisen ja tieteellisen kehityksen mahdollistamalla tavalla ja niin paljon kuin se on kohtuudella mahdollista”. (HE 262/2010 vp, s. 42)

son mukaisesti eli merkittävä muutos palvelun laadussa ilman palvelun tarjoamisen loppumista voisi myös olla merkittävä poikkeama. Koordinaatioryhmän mukaan käyttäjien määrällä muodostuisi luonnollisista ja oikeushenkilöistä, jotka ovat sopimussuhteessa palveluntarjoajaan. Määritelmän edellytys sopimussuhteesta on kuitenkin haastava mahdollisten tai tulevien käyttäjien poisjäämisen osalta. Poikkeaman kesto koordinaatioryhmän mukaan tulisi ymmärtää alkavan esimerkiksi tietomurron havaitsemista tai palvelun laatupoikkeamasta ja jatkuvan kunnes järjestelmät ovat täysin palautuneet tai järjestelmät on saatu puhdistettua esimerkiksi haittaohjelmasta. Maantieteellisen laajuuden osalta koordinaatioryhmä korostaa, että asianmukainen mittaustapa on määritettävä niille toimialoille, joissa maantiede on tärkeä. (NIS CG, 2018b, s. 10 ja 18-20)

NIS-direktiivin soveltamiseen liittyen ilmoituskynnyksen määrittelyyn on otettu kantaa useissa kirjallisuuslähteissä. ETSI organisaation NIS-direktiiviä koskevassa julkaisussa järjestö korostaa, että NIS-ilmoitukset koskevat palveluiden tarjonnan jatkuvuuteen liittyviä häiriöitä. Jatkuvuudella tarkoitettaisiin palveluiden saatavuutta ajan kuluessa, joka tukee palvelun käyttäjien mahdollisuuksia hyödyntää palveluita ja luottaa niiden saatavuuteen. Jatkuvuutta koskevalla muotoilulla tarkoitettaneen, että kriittisten palveluiden jatkuvuudessa ei ole aina häiriötä, vaikka käyttäjät eivät voisikaan palvelua käyttää, koska häiriö voi ilmetä myös käyttäjien puolella olematta mitenkään sidoksissa palvelun tarjontaan. ETSI mukaan ilmoitusvelvollisuus tulisi kapeasti rajata häiriöihin, jotka tosiasiassa vaikuttaa tietoturvallisuuteen. Tällöin esimerkiksi yrityksen asteelle jääneet tietomurrot, joilla mahdollisesti olisi ollut vaikutusta tietoturvallisuuteen, jäisivät ilmoitusvelvollisuuden ulkopuolelle. (ETSI, 2017, s. 13-14)

ETSI mukaan *merkittävällä vaikutuksella* ei ole yhtenäistä määritelmää vaan käsitteen sisältö saisi merkityksen kyseisen palvelun ja teknologisen arkkitehtuurin kontekstissa. Eri yhteyksissä käyttäjien suhteellinen määrä, maantieteellinen vaikutus ja kesto vaihtelevat. Käyttäjien määrän ja maantieteellisen alueen merkitys vaihtelee myös riippuen, minkä infrastruktuuritason palveluntarjonnasta puhutaan. Järjestö myös huomauttaa, että joissakin yhteyksissä käyttäjien määrän sijaan käyttötapahtumien laskeminen voi olla oleellisempi mittari, koska palveluntarjoajalla ei välttämättä ole tietoa loppukäyttäjien määrästä vaan esimerkiksi ainoastaan palvelua käyttävien organisaatioiden määrästä. (ETSI, 2017, s. 14)

ETSI suosituksen mukaan poikkeama olisi merkittävä, kun koko palvelu tai sen ydintoiminnallisuuden jatkuvuuteen tai saatavuuteen vaikutetaan eli edes pitkäaikainen häiriö tukitoiminnoissa ei tätä edellytystä täyttäisi. Mikäli ydintoimintojen häiriö käsitellään vaihtamalla automaattisesti varajärjestelmään, tällöin ilmoitusta ei tulisi vaatia, koska todellista ja havaittavaa vaikutusta palveluiden tarjoamisen jatkuvuuteen ei ilmene. (ETSI, 2017, s. 14)

Lähinnä teoreettinen merkittävän vaikutuksen tulkintaongelma voisi muodostua esimerkiksi pitkäkestoisen tietomurron ja sitä seuraavan virtuaalivaluutan laittoman louhinnan tai palvelunestohyökkäyksen tilanteessa, missä saatavuutta menetetään vähän kerrallaan, kunnes saatavuus on suurelta osin tai kokonaan menetetty. Ongelma tällöin on, että milloin hidas saatavuuden menetys

muodostaisi sellaisen merkittävän häiriön, josta tulisi ilmoittaa. Tämän lähinnä teoreettisen ongelman taustalla on First.org määritelmä saatavuudesta, jolla tietoturvallisuuden haavoittuvuusluokittelussa tarkoitetaan komponentin kuten verkkopalvelun (esim. selain, tietokanta, sähköposti) saatavuuden menetystä. Saatavuudella viitataan informaatioresurssin käytettävillä olemiseen, joten hyökkäykset verkkokapasiteettia, prosessorin syklejä tai levytilaa kohtaan kaikki vaikuttavat saatavuuteen komponenttitasolla. Vaikutus saatavuuteen on suuri, kun saatavuus menetetään täysin taikka kun saatavuus menetetään osittain, mutta saatavuuden menetyksellä on vakava vaikutus komponentin toimintaan. (First.org, 2019)

NIS-direktiivi ei siis edellytä, että esimerkiksi merenkulun turvallisuus voisi vaarantua vaan liikennemuodon turvallisuuden mahdollinen vaarantuminen on kansallinen rinnakkainen kriteeri ilmoituskynnykselle. Näkisin, että Suomessa käytetty muotoilu ilmoituskynnyksestä teoreettisesti laskee ilmoituskynnyksen direktiivin vähimmäisvaatimusta alemmas, mutta tätä olisi pidettävä ilmoitusvelvollisuuden tarkoituksen näkökulmasta positiivisena ja direktiivin johdantotekstin kohdan 47 mukaisesti nimenomaan sallittuna. Direktiivin sanamuodon näkökulmasta olisi ainakin teoriassa mahdollista, että poikkeamalla olisi merkittävää vähäisempi vaikutus yhteiskunnan keskeisen palvelun tarjoamiseen, mutta tästä huolimatta se voisi vaarantaa kyseisen liikkumismuodon turvallisuuden ja jäädä direktiivin mukaan ilmoittamatta.

Kansallisen lainsäädännön perusteella yhteenvetona voisi todeta, että toimijoiden on ilmoitettava viipymättä eli ilman aiheetonta viivytystä mistä tahansa tapahtumasta, joka tosiasiallisesti ja merkittävästi vaikuttaa toimijan riskienhallintavelvollisuuden kohteena oleviin viestintäverkkoihin ja tietojärjestelmiin ja voisi vaikuttaa kyseisen liikkumismuodon turvallisuuteen tai tosiasiallisesti merkittävästi vaikuttaa palvelun tarjoamisen jatkuvuuteen.

2.3 Liikenne- ja viestintäviraston toimivalta valvovana viranomaisena

Liikennejärjestelmän verkko- ja tietojärjestelmien turvallisuussääntelyä koskevan kappaleen viimeisessä alaluvussa vastataan kysymykseen: *Mahdollistaako NIS-direktiivin pohjalta annettu kansallinen verkko- ja tietojärjestelmien turvallisuussääntely tehokkaan ja tarkoituksenmukaisen liikennejärjestelmän keskeisten palveluiden tarjoajien valvonnan*. Kysymykseen vastataan kolmessa alakappaleessa, joista ensimmäisessä selvitetään, minkälaisia valvontavelvollisuuksia Liikenne- ja viestintävirasto Traficomille on säädetty ja minkälaisilla toimivaltuuksilla valvontaa voidaan tehdä. Valvontavelvollisuuksien selvittäminen on tärkeää, koska niiden tulisi kattaa edellä kappaleessa 2.1 määritetyt keskeisten palveluiden tarjoajat. Viranomaisen velvollisuuksien ja toimivaltuuksien kokonaisuuden selvittämisen yhteydessä arvioidaan, vastaavatko toimivaltuudet NIS-direktiivin vähimmäisvaatimuksia. Toimivaltuuksien ja velvollisuuksien selvittämisen jälkeen

loogisena jatkokysymyksenä toisessa alakappaleessa selvitetään, mitä toimintavaihtoja viranomaisella on käytettävissä, mikäli verkko- ja tietojärjestelmien turvallisuussääntelyn noudattamisessa havaitaan puutteita. Toimintavaihtoehtojen selvittämisen yhteydessä vastataan, mahdollistaako lainsäädäntö hallinnollisen pakon tai sanktioiden käytön. Kolmannessa alakappaleessa selvitetään, minkälaista määräystoimivaltaa valvoville viranomaisille on annettu. Määräystoimivallan osalta kolmannessa alakappaleessa pyritään edelleen vastaamaan, tulisiko toimivaltaisten viranomaisten hyödyntää määräystoimivaltaa tässä tutkimuksessa tunnistettujen sääntelyn ongelmakohtien selkeyttämiseksi.

2.3.1 Valvontavelvollisuudet ja toimivaltuudet

Suomen perustuslain 2.3 §:n mukaan ”[j]ulkisen vallan käytön tulee perustua lakiin. Kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia.” Tämä tarkoittaa, että viranomainen voi kohdistaa valvontaa vain niihin tahoihin, joiden valvonta on säädetty viranomaisen tehtäväksi. Lisäksi valvontaa voidaan tehdä vain niillä toimivaltuuksilla, jotka viranomaiselle on myönnetty. Toisaalta laadukkaan lainsäädännön näkökulmasta olisi optimaalista, että kaikkien yhteiskunnan keskeisten palveluiden verkko- ja tietojärjestelmien turvallisuusvelvoitteiden valvonta olisi säädetty jonkin viranomaisen tehtäväksi. Lisäksi olisi hyvä, että samankaltaisten velvoitteiden valvomiseksi olisi säädetty samankaltaiset toimivaltuudet eri yhteiskunnan aloilla. Verkko- ja tietojärjestelmien turvallisuussääntelyn valvonnan osalta toimivaltaisten viranomaisten oikeudet ja velvollisuudet ilmenevät sektorikohtaisesta lainsäädännöstä. Kappale rakentuu niin, että ensimmäisenä käsittelen Liikenne- ja viestintäviraston valvontavelvollisuudet ja toimivaltuudet raideliikenteessä, jonka jälkeen siirryn käsittelemään vesiliikennettä ja tieliikennettä sekä lopuksi käsittelen kaikille toimialoille samansisältöisiä toimivaltuuksia.

Raideliikenteessä Liikenne- ja viestintäviraston valvontavelvollisuudet ja toimivaltuudet verkko- ja tietojärjestelmien turvallisuusvelvoitteiden osalta eivät ole yksiselitteisesti ja selkeästi määritelty, joten valvontavelvollisuuksien kokonaisuuden hahmottamiseksi raideliikennelakia tulee tarkastella useita pykäliä yhdessä lukemalla. Lain 2 luvun 15 §:stä ilmenee Liikenne- ja viestintäviraston velvollisuudet raideliikenteen valvomiseksi. Verkko- ja tietojärjestelmien turvallisuuden näkökulmasta oleellisia ovat kohdat 3, 5 ja 6:

> Raideliikennelaki 15 § Rautatiejärjestelmän turvallisuuden ja yhteentoimivuuden valvonta
> Liikenne- ja viestintävirasto valvoo:
> – –
> 3) että rautatieliikenteen harjoittajat ja rataverkon haltijat toimivat turvallisuusjohtamisjärjestelmiensä mukaisesti ja että turvallisuusjohtamisjärjestelmät ovat 10 ja 11 §:n mukaisia;
> – –
> 5) varautumista poikkeusoloihin sekä häiriötilanteisiin rautatiejärjestelmässä varmistaakseen, että rautatieliikenteen harjoittaja ja rataverkon haltija toteuttavat turvallisuusjohtamisjärjestelmässään kuvaamiaan menettelyjä;

6) rataan kuuluvia ohjaus-, hallinta- ja merkinanto- sekä energia- ja infrastruktuuriosajärjestelmiä ja viraston on varmistettava niiden vaatimustenmukaisuus.
– –

Verkko- ja tietojärjestelmien turvallisuusriskien hallinnan valvonnan näkökulmasta kuudes kohta on selkein, koska kohdassa luetellaan erilaiset radan järjestelmät, joiden vaatimuksenmukaisuutta Liikenne- ja viestintäviraston tulee valvoa. Vaatimuksenmukaisuudella tässä yhteydessä tarkoitetaan ensisijaisesti nimenomaista EU:n rautatiesääntelyä, mutta sanamuoto ei sulje pois muun raideliikennelaista ilmenevän vaatimuksenmukaisuuden valvontaa. Siltä osin, kun nämä järjestelmät tunnistetaan edellä riskienhallintavelvollisuutta koskevan kappaleen 2.2.1 mukaisiksi järjestelmiksi, yhteiskunnan keskeisen palveluntarjoajan riskienhallintavelvollisuus sekä Liikenne- ja viestintäviraston valvontavelvollisuus symmetrisesti vastaavat toisiaan. Kohdan osalta on erikseen syytä korostaa, että valvontavelvollisuutta ei rajata tiettyyn rautatietoimijaan vaan valvontavelvollisuus kohdistuu itse järjestelmiin riippumatta siitä, kuka järjestelmän tietoturvallisuusvelvoitteiden hallinnasta vastaa.

Valvontatehtävien luettelon kohtien 3 ja 5 keskiössä on rautatieliikenteenharjoittajien ja rataverkon haltijoiden turvallisuusjohtamisjärjestelmän valvonta. Sanamuodon mukaisesti turvallisuusjohtamisjärjestelmä ei suoraan koske liikenteenohjauspalveluiden tarjoajaa, koska sitä ei ole kohdassa mainittu. Lain 10 §:ssä säädetään siitä, mikä on turvallisuusjohtamisjärjestelmä ja mitä sen tulee sisältää. Verkko- ja tietojärjestelmien turvallisuusvelvoitteiden näkökulmasta oleellista on, että turvallisuusjohtamisjärjestelmällä rautatieliikenteen harjoittajan sekä rataverkon haltijan on varmistettava, että rautatiejärjestelmässä noudatetaan kansallisia oikeussääntöjä. Raideliikennelaissa kansallisilla oikeussäännöillä ensisijaisesti tarkoitetaan EU:n rautatiesääntelyn mahdollistamaa kansallista liikkumisvaraa säädellä kansallisesti sellaisia yksityiskohtia, mitä EU-tasolla ei ole säännelty. Kuitenkin sanamuotoa laajasti tulkiten kansallisten oikeussääntöjen voidaan tässä yhteydessä ymmärtää kattavan myös raideliikennelaista ilmenevien verkko- ja tietojärjestelmien turvallisuusvelvoitteiden noudattamisen. Kun 10 §:n mukaista rataverkon haltijan velvollisuutta turvallisuusjohtamisjärjestelmällä osoittaa verkko- ja tietojärjestelmien turvavelvoitteiden noudattaminen luetaan yhdessä raideliikennelain 136 §:n kanssa, jonka mukaan rataverkon haltija vastaa hallinnoimansa rataverkon liikenteenohjauksen järjestämisestä, voidaan rataverkon haltijan velvollisuutena katsoa olevan turvallisuusjohtamisjärjestelmällä osoittaa, että myös liikenteenohjauspalvelun tarjoaja noudattaa verkko- ja tietojärjestelmien turvavelvoitteita 169 §:n mukaisesti. Edellä kappaleessa 2.1.1 raideliikenteen keskeisten toimijoiden määrittelyssä käsiteltiin raideliikenteenohjauspalveluiden ulkoistamista edelleen VR Yhtymä Oy:lle ja Destia Rail Oy:lle. Näiden yritysten ollessa raideliikenteen harjoittajia heitä koskevat turvallisuusjohtamisjärjestelmään liittyvät velvoitteet ja siten liikenteenohjauksen tietoturvavelvoitteiden huomiointi osana ulkoistettua liikenteenohjauspalvelua.

Raideliikennettä koskevien valvontavelvollisuuksien selvittämisen jälkeen on hyvä tarkastella, minkälaisilla toimivaltuuksilla valvontaa voi tehdä. Raideliikennelain 16 §:stä ilmenevät Liikenne- ja viestintäviraston toimivaltuudet valvontatehtävien hoitamiseksi. Valvontaa on mahdollista tehdä ennakkoilmoituksen perusteella tai ennalta ilmoittamatta. Valvonnan tekeminen ei edellytä mitään erityistä syytä kuten häiriöstä ilmoittamista tai vihjettä laiminlyönnistä. Valvonnassa virastolla on oikeus hyödyntää asiantuntijan apua, mikä tietoturvallisuuteen liittyvissä kysymyksissä voisi tarkoittaa esimerkiksi Kyberturvallisuuskeskuksen tai yksityisten tietoturvayritysten asiantuntemuksen hyödyntämistä. Konkreettisesti valvontatoimivaltuus on pykälässä ryhmitelty kolmeen kokonaisuuteen: Pääsyoikeus tiloihin ja laitteisiin, henkilöstön valvonta sekä tietojen saanti.

Valvonnan toteuttamiseksi virastolla on oikeus ”päästä valvonnan edellyttämässä laajuudessa rautatieliikenteen harjoittajan, rataverkon haltijan, liikenteenohjauspalvelua harjoittavan yhtiön tai yhteisön ja muun rautatiejärjestelmään kuuluvaa tehtävää suorittavan yrityksen toimitiloihin ja muihin tiloihin, laitteistoihin ja laitteisiin lukuun ottamatta pysyväisluonteiseen asumiseen käytettäviä tiloja” (Raideliikennelaki 16.2 §:n 1 kohta) sekä valvoa näiden toimijoiden henkilöstön toimintaa (16.2 §:n 2 kohta). Toimivaltuudesta on syytä ensinnäkin korostaa, että (raideliikenteen) liikenteenohjauspalvelut on toimivaltuudessa nimenomaisesti mainittu, vaikka velvollisuutta valvoa liikenteenohjauspalvelua ei ole suoraan ja yksiselitteisesti raideliikennelakiin kirjattu. Lisäksi toimivaltuus koskee myös muun rautatiejärjestelmään kuuluvan tehtävää suorittavan yrityksen tiloja. Kun verkko- ja tietojärjestelmien turvallisuudesta huolehtiminen on raideliikennelaissa säädetty osaksi rautatiejärjestelmään kuuluvia tehtäviä, toimivaltuuden on mahdollista tulkita kattavan oikeuden päästä esimerkiksi toimijan tietoturvallisuudesta vastaavan yrityksen tiloihin ja laitteistoihin. Toimivaltuus kattaa tiloihin liittyvän pääsyoikeuden lisäksi pääsyn laitteistoihin ja laitteisiin. Tietoturvallisuuden valvomisen näkökulmasta virastolla olisi täten oikeus päästä tarkkailemaan laitteiston toimintaa ja tätä kautta varmistua esimerkiksi tietoturvapäivitysten ajantasaisuudesta taikka seurata kyseisen laitteen verkkoliikennettä. Toimivaltuus ei kuitenkaan vaikuta mahdollistavan seurantaa tai tarkkailua aktiivisempia valvontatoimenpiteitä laitteistoissa kuten esimerkiksi tietoturvahaavoittuvuuksien skannausta taikka järjestelmien tietoturvahaavoittuvuuksien selvittämistä penetraatiotestauksella (tunkeutumistestauksella). Toimivaltuus mahdollistaa myös henkilöstön toiminnan valvonnan, mikä voisi merkitä esimerkiksi toimijan tietoturvahenkilöstön toiminnan valvomista harjoituksen yhteydessä tai oikeassa tilanteessa sekä esimerkiksi organisaation johdon valvontaa merkittävää tietoturvahäiriötä käsiteltäessä.

Toimivaltuus kattaa myös oikeuden saada nähtäväksi salassapitosäännösten estämättä valvontatehtävän kannalta tarpeelliset asiakirjat (16.2 §:n 3 kohta). Raideliikennelain erikoisuutena voi pitää sitä, että samassa laissa valvontatehtäviä varten on kaksi eri tiedonsaantipykälää. Edellä mainittu tiedonsaantioikeus vaikuttaisi olevan laajempi kuin raideliikennelain 189 §:n tiedonsaantioikeus,

jonka mukaan Liikenne- ja viestintävirastolla on oikeus saada maksutta ja liikesalaisuuksien estämättä rautatieliikenteen harjoittajalta tai rataverkon haltijalta tiedot, joita tarvitaan raideliikennelain 2 luvussa tarkoitettua valvontaa varten. Kaksi eri tiedonsaantioikeuspykälää muodostavat erikoisen kokonaisuuden: Rautatieliikenteen harjoittajilta sekä rataverkon haltijoilta Liikenne- ja viestintäviraston on mahdollista saada tietoja sekä 16.2 §:n 3 kohdan että 189 §:n nojalla. Jälkimmäinen pykälä ei kuitenkaan mahdollista tietojen saamista liikenteenohjauspalvelun tarjoajalta, koska tätä ei pykälässä mainita. Tietojen saanti liikenteenohjauspalvelun tarjoajalta on kuitenkin mahdollista 16.2 §:n 3 kohdan nojalla, kun se on tarpeen valvontatehtävän hoitamiseksi. Kuitenkin edellä tuotiin esille, että raideliikennelaissa ei ole yksiselitteisesti ja selkeästi säädetty Liikenne- ja viestintävirastolle tehtäväksi valvoa liikenteenohjauspalveluiden tarjoajan verkko- ja tietojärjestelmien turvallisuusvelvoitteiden noudattamista. Tällöin 16.2 §:n 3 kohdan mukaisen tietojensaantioikeuden kohdistaminen liikenteenohjauspalveluiden tarjoajaan voi johtaa tulkinnanvaraisiin tilanteisiin.

Vesiliikenteessä VTS-palveluiden kohdalla on selkeää, että Liikenne- ja viestintävirastolla on velvollisuus valvoa VTS-palveluntarjoajan tietoturvallisuusvelvoitteiden noudattamista. Alusliikennepalvelulain 28.1 §:n mukaan lain noudattamisen ylin valvonta kuuluu LVM:lle ja toisen momentin mukaan lain noudattamisen valvonta kuuluu myös Liikenne- ja viestintävirastolle. Lisäksi saman pykälän neljännessä momentissa erikseen täsmennetään viraston valvontavelvollisuutta.

> ”Liikenne- ja viestintäviraston on arvioitava 16 §:n 5 momentissa tarkoitetun [*viestintäverkkojen ja tietojärjestelmien]* riskienhallinnan vaikutuksia merenkulun turvallisuuteen. Liikenne- ja viestintävirasto voi velvoittaa ryhtymään korjaaviin toimenpiteisiin merenkulun turvallisuuteen kohdistuvan merkittävän riskin poistamiseksi. Velvoitteen tehosteeksi voidaan asettaa uhkasakko. Uhkasakosta säädetään uhkasakkolaissa.”

Verkko- ja tietojärjestelmien turvallisuuden näkökulmasta osittain päällekkäisenä valvontavelvollisuutena Liikenne- ja viestintävirastolla on alusliikennepalvelulain 19 a §:n mukaan valvoa, että VTS-palveluntarjoaja valmistelee etukäteen normaaliolojen häiriötilanteissa tapahtuvaa toimintaa. Kohtaa voi mielestäni tulkita niin, että normaaliolojen häiriötilanteena voidaan pitää merkittävää tietoturvallisuuteen liittyvää häiriötä.

Alusliikennepalvelulaissa Liikenne- ja viestintävirastolle ei ole säädetty varsinaisia toimivaltuuksia valvonnan toteuttamiseksi. Käytännössä ainoaksi valvonnassa käytettäväksi toimivaltuudeksi jää toimintakäsikirjan hyväksyminen. Alusliikennepalvelulain 19.1 §:n mukaan VTS-palveluntarjoaja ylläpitää Liikenne- ja viestintäviraston hyväksymää toimintakäsikirjaa, jossa määritellään VTS-keskuksen tehtävät, toimenpiteet ja normaaliolojen häiriötilanteisiin varautuminen. Velvollisuus hyväksyttää toimintakäsikirjan Liikenne- ja viestintävirastolla käytännössä merkitsee, että virastolla on toimivalta olla hyväksymättä toimintakäsikirjaa, mikäli viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden riskienhallinta ei olisi riittävällä tasolla.

Kuten vesiliikenteessä VTS-palveluiden osalta, myös satamien verkko- ja tietojärjestelmien turvallisuuden valvonta on täsmällisesti säädetty Liikenne- ja viestintäviraston tehtäväksi. Kuitenkin satamien turva-arviointiin liittyvä velvoite vaikuttaisi laajentavan Liikenne- ja viestintäviraston velvollisuuksia. Satamia koskevan turvatoimilain mukaan Liikenne- ja viestintävirasto on toimivaltainen viranomainen (2.1 §:n 1 kohta). Toimivaltaisen viranomaisen tehtävänä on valvoa, että turvatoimilain mukaisia säädöksiä noudatetaan (3.1 §). Liikenne- ja viestintäviraston tehtävänä on suorittaa turvatoimilaissa virastolle säädetyt tehtävät (4.1 §:n 9 momentti).

Kuitenkin alusliikennepalvelulaista poiketen turvatoimilaissa Liikenne- ja viestintävirastolle on säädetty toimivaltuudet valvonnan toteuttamiseksi. Toimivaltaisella viranomaisella on oikeus saada maksutta nähtäväkseen sekä jäljennöksiä turvatoimilain tavoitteiden toteuttamisen kannalta tarpeellisista asiakirjoista ja muusta aineistosta, joita satamanpitäjän on pidettävä tai säilytettävä (16.1 §). Satamanpitäjän velvollisuutta pitää tai säilyttää verkko- ja tietojärjestelmien turvallisuuden riskienhallintaan liittyviä asiakirjoja ei edellä mainitulla tietojensaantipykälällä laajenneta eli toimivaltaisen viranomaisen tiedonsaantioikeuden laajuus käytännössä vastaa satamanpitäjän riskienhallinnan dokumentaatiovelvollisuutta (ks. edellä kappale 2.2.1.4 dokumentaatiovelvollisuus).

Satamien verkko- ja tietojärjestelmien turvallisuuden hallintaan liittyvänä tulkinnanvaraisena erityispiirteenä on turvatoimilain mukainen turva-arviointi. Liikenne- ja viestintäviraston tehtävänä on suorittaa satamien turva-arvioinnit ja hyväksyä satamien turvallisuussuunnitelmat (4.1 §:n 1 kohta). Turva-arvioinnissa on asianmukaisesti huomioitava satamaturvadirektiivin liitteen 1 vaatimukset (7 a §:n 2 momentti). Satamaturvadirektiivin liitteen 1 mukaan turva-arvioinnissa on määritettävä ja arvioitava sellainen infrastruktuuri, jota on tärkeä suojella. Lisäksi on määritettävä infrastruktuurin heikkoudet, siihen kohdistuvat uhkat ja niiden todennäköisyys sekä tarvittavat vastatoimet. Satamaturvadirektiivi on säädetty vuonna 2005 eli kymmenen vuotta ennen NIS-direktiivin valmistelua aikana, jolloin satamien verkko- ja tietojärjestelmien turvallisuuteen kohdistuvaa riskienhallintaa ei oletettavasti korostettu. Direktiivin sanamuoto on kuitenkin väljästi muotoiltu, joten sitä on mahdollista tulkita niin, että Liikenne- ja viestintäviraston velvollisuutena turva-arvioinnissa olisi määrittää satamien verkko- ja tietojärjestelmien turvallisuuden riskienhallinnan suuret linjat, jonka pohjalta satama laatisi turvasuunnitelman (7 b §). Tähän velvollisuuteen satamaturvadirektiivin liitteen 1 sanamuodon mukaan voisi kuulua ainakin verkko- ja tietojärjestelmien turvallisuuden riskienhallinnan kohteena olevien järjestelmien määrittäminen sekä edellä kappaleessa 2.2.1 käsiteltyjen asianmukaisten ja oikeasuhtaisen teknisten ja organisatoristen keinojen määrittäminen niin, että satama kykenee suojautumaan tietyllä varmuudella palvelujen saatavuutta vaarantavilta toimilta. Mikäli edellä esitetty tulkinta Liikenne- ja viestintäviraston velvollisuudesta hyväksytään, satamien verkko- ja tietojärjestelmien turvallisuuden valvontaan voi muodostua ongelmallinen tilanne, jossa valvova viranomainen voi joutua osittain valvomaan itseään. Liikenne- ja viestintäviras-

ton tulee valvoa, että satamien verkko- ja tietojärjestelmien turvallisuuden riskienhallinta on riittävä, mutta samalla virasto turva-arvioinnissa osallistuu riittävän riskienhallintatason määrittämiseen. Mikäli merkittävän tietoturvahäiriön tapahduttua jälkikäteen Liikenne- ja viestintävirasto päätyisi lopputulemaan, että tietoturvariskienhallinta ei tosiasiallisesti ollut riittävällä tasolla, tällöin virasto samalla toteaisi, että sen itsensä tekemä turva-arviointi ei tosiasiallisesti ollut riittävä. Toisaalta satamien näkökulmasta turva-arvioinnin tulkinnanvaraisuus suhteessa verkko- ja tietojärjestelmien turvallisuussääntelyyn luo satamille hyödyllisen tilanteen, missä satama voi halutessaan vaatia Liikenne- ja viestintävirastolta laadukasta turva-arviointia, jolloin turva-arvioinnin tuloksia hyödyntävän sataman itsensä ei välttämättä tarvitse kohdentaa niin paljon resursseja tietoturvallisuuden riskienhallinnan määrittelytyöhön.

Tieliikenteen puolella liikenteen palveluista annetun lain mukaan Liikenne- ja viestintäviraston tehtävänä on valvoa ”tämän lain sekä sen nojalla annettujen säännösten, määräysten ja päätösten noudattamista, jollei tässä laissa muuta säädetä” (178.1 §). Koska laissa ei verkko- ja tietojärjestelmien turvallisuuden valvonnasta erikseen muuta säädetä, voidaan pitää selvänä, että valvontatoimivalta kuuluu Liikenne- ja viestintävirastolle. Valvontatehtävän hoitamiseksi Liikenne- ja viestintävirastolle on annettu toimivalta päästä toimipaikkojen tiloihin tarkastusten suorittamiseksi (196.1 §), minkä lisäksi tarkastuksen kohteena oleva palveluntarjoaja on velvollinen avustamaan virastoa tarkastuksessa sekä tarjoamaan tiloja ja laitteita tarkastuksen toteuttamiseksi (196.2 §). Virastolla on välttämättömissä tilanteissa oikeus ottaa haltuunsa aineistoa tai jäljentää se (196.3 §). Virastolla on myös omalla kustannuksellaan (196.5 §) oikeus käyttää valvonnassa ulkopuolisen perehtyneen asiantuntijan apua, mutta viraston tulee valvoa ulkopuolisen asiantuntijan toimintaa ja vastuu valvonnasta säilyy virastolla (196.4 §). Hallituksen esityksessä tarkennetaan, että ulkopuolisen asiantuntijan käytössä ei ole kysymys valvonnan ulkoistamisesta vaan sellaisen teknisen erityisosaamisen hankkimisesta, jota viranomaisella ei ole muutoin käytettävissä. (HE 145/2017 vp, s. 245) Selvyyden vuoksi on syytä vielä todeta, että liikenteen palveluista annetun lain 25 luku mahdollistaa useiden viranomaista tukevien avustavien tehtävien ulkoistamisen, mutta verkko- ja tietojärjestelmien turvallisuuden valvontaan liittyviä tehtäviä virasto ei lain mukaan voi ulkoistaa (209-211 §). Valvonnan toteuttamiseksi virastolla on oikeus saada salassapitosäännösten estämättä, viipymättä, maksutta ja viranomaisen pyytämässä muodossa valvontatehtävän suorittamiseksi välttämättömät tiedot (197 §:n 1-2 momentit). Edellä mainitun valvontaviranomaisen yleisen tiedonsaantioikeuden lisäksi on osittain päällekkäisesti säädetty pelkästään liikenteenohjauspalveluita koskeva tiedonsaantioikeus: ”Viranomaisella on oikeus liike- ja ammattisalaisuuden estämättä saada liikenteen ohjaus- ja hallintapalveluiden tarjoajalta lakisääteisen tehtävän hoitamiseksi tarvittavat tiedot” (147.1 §). Toimivaltuuksiin liittyen on lopuksi hyvä selventää, että tieliikenteen ohjaus- ja hallintapalveluiden tarjoaja on velvollinen pitämään toimintakäsikirjaa, joka kattaa ”palveluntarjoajan toiminnan ja teknisten järjestelmien ylläpitämiseen liittyvät tehtävät ja toimenpiteet sekä varautuminen palvelun ylläpitämiseen poikkeustilanteissa” (138.3 §). Toimintakäsikirjaa

koskeva velvoite on tarkoitettu samankaltaiseksi kuin vesiliikenteessä VTS-palveluiden osalta. (HE 34/2018 vp, s. 85) Vaikka velvoite on samankaltainen, tieliikenteessä toimintakäsikirjan ei tarvitse kattaa varautumista normaaliolojen häiriötilanteisiin eikä laki vaadi toimintakäsikirjan hyväksyttämistä Liikenne- ja viestintävirastolla. Tämän takia tieliikenteen ohjaus- ja hallintapalveluiden toimintakäsikirjaa ei voi mieltää samankaltaiseksi tietoturvallisuuden valvonnan toimivaltuudeksi ja työkaluksi kuten vesiliikenteen VTS-palveluiden kohdalla.

Edellä käsiteltyjä valvontavelvollisuuksia ja toimivaltuuksia on mahdollista hyödyntää sekä ennen merkittävän tietoturvahäiriön syntymistä että sen jälkeen. Näiden toimivaltuuksien lisäksi NIS-direktiivin velvoitteista johtuen kaikkien liikennöintimuotojen osalta on sektorikohtaiseen lainsäädäntöön lähes samansisältöisesti kirjattu, että merkittävän tietoturvallisuuteen liittyvän häiriön tapahduttua ja rataverkon haltijan, (raide)liikenteenohjauspalvelun tarjoajan, VTS-palveluntarjoajan, satamanpitäjän, (tie)liikenteen ohjaus- ja hallintapalveluiden tarjoajan taikka älykkään liikennejärjestelmän ylläpitäjän siitä ilmoitettua, Liikenne- ja viestintäviraston velvollisuutena on arvioida, koskeeko häiriö muita EU-jäsenvaltioita ja mikäli koskee, tarvittaessa ilmoittaa asiasta kyseisille valtioille. (Raideliikennelaki 169.4 §, Alusliikennepalvelulaki 18 a.3 §, Turvatoimilaki 7 f.3 §, Laki liikenteen palveluista 140.4 ja 161.4 §.) Raideliikennelain osalta arviointi- ja ilmoitusvelvoite kattaa EU-jäsenvaltioiden lisäksi ETA-jäsenvaltiot eli EU-jäsenvaltioiden lisäksi vaikutukset Norjaan, Islantiin ja Liechtensteiniin tulevat myös arvioitavaksi (raideliikennelaki 169.4 §). Arvioinnin ulottaminen ETA-jäsenvaltioihin ylittää direktiivin vähimmäisvaatimuksen ja on erikoinen, koska NIS-direktiiviä ei ole säädetty ETA-jäsenvaltioille merkitykselliseksi, vaikkakin Norja ja Islanti ovat pitäneet säädöstä ETA-valtioille oleellisena ja hyväksyttävänä. (Norwegian Ministeries, 2019, s. 21)

Yhteenvetona Liikenne- ja viestintäviraston verkko- ja tietojärjestelmien turvallisuuden valvontavelvollisuuksista voi todeta, että vesi- ja tieliikenteessä viraston valvontavelvollisuus ilmenee selkeästi sektorikohtaisesta lainsäädännöstä, joskin satamien kohdalla turva-arvioinnin voidaan katsoa ulottuvan perinteistä valvontaa pidemmälle kohti riskienhallinnan selvittämis- ja määrittelyvelvoitetta. Raideliikennelaista selkeästi ilmenee viraston velvollisuus valvoa, että Väylävirasto rataverkon haltijana noudattaa verkko- ja tieturvallisuusvelvollisuuksia. Kuitenkin raideliikenteen liikenteenohjauspalveluiden osalta asia ei ole näin selkeä. Selvää on, että virastolla on liikenteenohjauspalveluihin kohdistuva valvontavelvollisuus siltä osin, kun verkko- ja tietojärjestelmien turvallisuusvelvoite kohdistuu radan ohjaus-, hallinta- ja merkinanto-, energia- tai infrastruktuuriosajärjestelmään. Verkko- ja tietojärjestelmien turvallisuuden valvontavelvollisuus on myös siltä osin, kun rautatieliikenteenharjoittaja huolehtii liikenteenohjauksesta Fintrafficin ulkoistaman liikenteenohjauksen osalta. Raideliikennelaissa Liikenne- ja viestintävirastolle ei ole kuitenkaan säädetty suoraa velvollisuutta valvoa, että Fintraffic Raide Oy noudattaa sille raideliikennelaissa säädettyjä verkko- ja tietojärjestelmien turvallisuuden riskienhallinta- ja ilmoittamisvelvollisuuksia. Liikenne- ja viestintävirastolla on kuitenkin välillinen vel-

voite valvoa raideliikenteen liikenteenohjauspalveluiden verkko- ja tietojärjestelmien turvallisuusvelvoitteita, koska Liikenne- ja viestintävirasto valvoo Väyläviraston ja Väyläviraston tulee turvallisuusjohtamisjärjestelmällä osoittaa liikenteenohjauspalveluntarjoajan noudattavan näitä velvoitteita. Liikenne- ja viestintäviraston suoran raideliikenteen liikenteenohjauspalveluihin kohdistuvan valvontavelvollisuuden puute on kuitenkin ongelmallinen, koska ilman lakiin perustuvaa valvontavelvollisuutta ei virasto voi hyödyntää sille säädettyjä valvontatehtävään sidottuja valvontatoimivaltuuksia.

Mikäli NIS-direktiivin pohjautuvia Liikenne- ja viestintäviraston valvontavelvollisuuksia voi pääpiirteittäin luonnehtia yhtenäiseksi ja symmetriseksi suhteessa velvollisuuteen noudattaa verkko- ja tietojärjestelmien turvallisuussääntelyä, toimintavaltuuksien osalta tilanne on hyvin erilainen. Voidaan pitää jopa yllättävänä, että hyvin samankaltaisten velvollisuuksien valvomiseksi annetut toimivaltuudet poikkeavat näin suuresti. Hieman yleistäen voi luonnehtia, että Liikenne- ja viestintäviraston toimivaltuudet ovat selkeästi laajimmat raideliikenteessä ja vähäisimmät vesiliikenteessä VTS-palveluiden osalta. Raideliikenteessä viraston toimivaltuudet kattavat pääsyn tiloihin ja laitteisiin ilman ennakkoilmoitusta, oikeuden hyödyntää ulkopuolista asiantuntijaa, oikeuden valvoa henkilöstöä sekä tiedonsaantioikeuden. Tieliikenteessä toimivaltuudet kattavat oikeuden päästä toimitiloihin, saada tarkastuksen kohteelta apua, hyödyntää ulkopuolista asiantuntijaa sekä oikeuden saada tietoa. Satamien kohdalla ainoa selkeä toimivaltuus on tiedonsaantioikeus, mutta turva-arvioinnin toteuttamisen voi ymmärtää luonnollisesti kattavan myös oikeuden päästä arvioitavaan kohteeseen ja havainnoida kaikkea toimintaa kohteessa. VTS-palveluiden osalta Liikenne- ja viestintävirastolle ei ole säädetty samankaltaisia varsinaisia valvontatoimivaltuuksia kuten muissa liikennöintimuodoissa, mutta VTS-palveluiden kohdalla toimivaltuutena on hyväksyä tai olla hyväksymättä VTS-palveluntarjoajan ylläpitämää toimintakäsikirjaa.

Kappaleen lopuksi vielä arvioin, vastaavatko edellä käsitellyt Liikenne- ja viestintäviraston valvontavelvollisuudet ja toimivaltuudet NIS-direktiivin vähimmäistasoa. NIS-direktiivin 15(1) artiklan mukaan toimivaltaisille viranomaisille on varmistettava ”tarvittavat valtuudet ja keinot arvioida, noudattavatko keskeisten palvelujen tarjoajat 14 artiklan mukaisia velvollisuuksiaan, sekä tämän vaikutuksia verkko- ja tietojärjestelmien turvallisuuteen.” Viittauksella 14 artiklaan tarkoitetaan edellä käsiteltyjä riskienhallinta- ja ilmoitusvelvollisuutta. On perusteltua tulkita 15(1) artiklan vähintään velvoittavan jäsenvaltioita varmistamaan, että yhteiskunnan keskeisten palveluiden tarjoajien verkko- ja tietoturvallisuuden valvonta on säädetty toimivaltaisen viranomaisen tehtäväksi. Vesi- ja tieliikennesektoreilla Suomen lainsäädäntö täyttää direktiivin vähimmäisvaatimuksen, mutta raideliikenteen osalta kysymys on tulkinnanvarainen. Kuten edellä kappaleessa esitettiin, raideliikennelain mukana Liikenne- ja viestintävirastolla on toimivalta ottaa vastaan raideliikenteenohjauspalvelun tarjoajalta verkko- ja tietojärjestelmien turvallisuuteen liittyviä ilmoituksia häiriöistä, valvoa tiettyjä radan toimintaan liittyviä järjestelmiä sekä välillisesti Väyläviras-

ton kautta valvoa liikenteenohjauspalvelun tarjoajaa. Liikenne- ja viestintävirastolle ei kuitenkaan ole säädetty suoraa liikenteenohjauspalvelun tarjoajan verkko- ja tietojärjestelmien turvallisuuden valvontavelvollisuutta, joten kysymyksen tulkinnanvaraisuudesta huolimatta vaikuttaisin enemmänkin siltä, että raideliikennelaki ei tältä osin täysin saavuttaisi NIS-direktiivin vähimmäisvaatimusta.

NIS-direktiivin 15(2) artiklassa määritellään vähimmäistoimivalta, joka jäsenvaltioiden tulee toimivaltaisille viranomaisille myöntää. Kohdan mukaan toimivaltaisilla viranomaisilla tulee olla tarvittava tietojensaantioikeus verkko- ja tietojärjestelmien turvallisuuden arvioimiseksi, joka kattaa tiedonsaannin turvallisuusohjeista, turvallisuusohjeiden täytäntöönpanoa osoittavasta näytöstä sekä turvallisuustarkastuksien tuloksista ja tuloksia tukevasta näytöstä. Tiedonsaantioikeuksista on säädetty raide- ja tieliikenteessä sekä satamien osalta, mutta alusliikennepalvelulaista toimivaltuus saada tietoja puuttuu. Tältä osin on mahdollista todeta, että alusliikennepalvelulaki ei täytä direktiivin vähimmäisvaatimusta, koska Liikenne- ja viestintävirastolla ei ole selkeää tiedonsaantioikeutta meriliikenteenohjauspalvelun tarjoajan verkko- ja tietojärjestelmien turvallisuuden arvioimiseksi.

2.3.2 Toimintavaihtoehdot puutteita havaittaessa ja häiriöiden tapahduttua

Tässä alakappaleessa selvitetään, mitä toimintavaihtoja Liikenne- ja viestintävirastolla on käytettävissä, mikäli verkko- ja tietojärjestelmien turvasääntelyn noudattamisessa havaitaan puutteita tai häiriöistä ilmoitetaan. Toimintavaihtoehtojen selvittämisen yhteydessä vastataan, mahdollistaako lainsäädäntö hallinnollisen pakon tai sanktioiden käytön. Kappaleen lopuksi myös arvioidaan, vastaavatko Liikenne- ja viestintävirastolle säädetyt toimintavaihtoehdot ja sanktiovaltuudet NIS-direktiivin vähimmäisvaatimuksia. Näkökulmasta riippuen kappaleessa käsiteltävät toimintavaihtoehdot voidaan nähdä osana valvontatoimivaltuuksia, mutta ne voidaan mieltää muodostavan myös oman esitysteknisen kokonaisuuden, koska niiden käyttö mahdollistuu vasta puutteiden tai häiriön havaitsemisen jälkeen. Tässä yhteydessä on syytä korostaa, että puutteet tietoturvariskienhallinnassa ja tietoturvahäiriöt eivät aina ole sidoksissa toisiinsa. Puutteita voi löytyä ilman, että niistä koskaan aiheutuu häiriötä. Häiriö ei välttämättä ole syy-yhteydessä riskienhallinnan puutteeseen, mutta häiriön syntymisen jälkeen myös riskienhallinnan puutteita voidaan havaita.

Raideliikenteessä Liikenne- ja viestintävirastolla on käytettävissä suhteellisen laaja keinovalikoima verkko- ja tietojärjestelmien turvasäännösten noudattamisen tehostamiseksi sekä häiriöihin puuttumiseksi. Raideliikennelaki mahdollistaa huomautusten ja varoitusten (178 §), toiminnanharjoittajia koskevien määräysten, velvoitteiden sekä uhkasakon (179 §) määräämisen. Raideliikennelain 178 §:n antaa Liikenne- ja viestintävirastolle toimivallan antaa huomautuksen tai kirjallisen varoituksen raideliikennelain tai sen nojalla annetun säännöksen vastaisesti toimivalle. Verkko- ja tietojärjestelmien turvavelvoitteiden ollessa osa raideliikennelakia huomautus tai varoitus voidaan antaa myös näiden sääntöjen rikkomisesta. Mikäli Liikenne- ja viestintävirasto antaisi tarkempia verkko- ja

tieturvallisuutta koskevia määräyksiä, huomautus ja varoitustoimivalta koskisi myös näiden määräysten noudattamista. Varoitus voidaan antaa suoraan huomautusta antamatta, mikäli huomautusta ei kokonaisuutena pidetä riittävänä. Huomautus tai varoitus voidaan antaa rautatieliikenteen harjoittajalle, rataverkon haltijalle, 159 §:ssä tarkoitetulle toiminnanharjoittajalle tai muulle tässä laissa tarkoitetulle toiminnanharjoittajalle. Toimivaltuus kattaa kaikki raideliikennelaissa tarkoitetut verkko- ja tietojärjestelmien turvallisuusvelvoitteiden kohteena olevat toiminnanharjoittajat.

Mikäli toiminnanharjoittaja huomautuksesta tai varoituksesta huolimatta toimii raideliikennelain tai sen nojalla annettujen säädösten vastaisesti, Liikenne- ja viestintävirasto voi 179 §:n mukaisesti määrätä ”toiminnanharjoittajan korjaamaan virheensä tai laiminlyöntinsä sekä asettaa tälle velvoitteita taikka kieltää toimenpiteen”. Määräyksen tehosteeksi on mahdollista asettaa uhkasakkolain mukainen uhkasakko, uhata keskeyttää toiminta tai teetättää toimenpide asianomaisen kustannuksella. Tämän 179 §:n mukaisen toimivaltuuden käyttämisen edellytyksenä on, että toiminnanharjoittajalle on jo annettu vähintään yksi huomautus tai varoitus kyseisestä asiasta. Virheen tai laiminlyönnin korjaamiseen velvoittamisen ilmeisimmät sovellustapaukset voisivat kohdistua esimerkiksi tietoturvallisuuden teknisiin näkökulmiin tai puutteisiin tietoturvariskienhallinnan johtosuhteissa, mutta tietoturvallisuuden riskienhallinnan laiminlyömisen voi myös tulkita kattavavan esimerkiksi tietoturvallisuudesta huolehtivan henkilöstön alimitoittamisen tai heidän puutteellisen resursoinnin.

Raideliikennelaki 180 § antaa Liikenne- ja viestintävirastolle oikeuden keskeyttää raideliikenne tai rajoittaa raideliikennettä taikka sitä uhkaava tai siihen vaikuttava toimenpide tai tapahtuma. Toimivaltuuden käyttö on mahdollista normaaliolojen vakavassa häiriötilanteessa taikka mikäli raideliikennejärjestelmän turvallisuus, ihmishenki tai terveys ovat uhattuina. Pykälän säätämisen taustalla on covid-19 pandemian aiheuttamat muutostarpeet ja valmiuslain käytön välttäminen. (HE 113/2020 vp, s. 23-24) Verkko- ja tietojärjestelmien turvallisuussääntelyn näkökulmasta käsite normaaliolojen vakava häiriötilanne voidaan ymmärtää vakavuudeltaan samankaltaiseksi kuin edellä käsitelty merkittävästä tietoturvahäiriöstä ilmoittamisen kynnys. Tällöin Liikenne- ja viestintävirastolla olisi raideliikenteen rajoittamisen lisäksi oikeus puuttua tietoturvallisuuden häiriön juurisyihin keskeyttämällä tai rajoittamalla häiriön taustalla olevaa toimenpidettä tai muuta tapahtumaa. Toimivaltuutta voi luonnehtia jopa epämääräisen laajaksi, koska sen rajat eivät ole tarkkarajaiset ja erityisesti ilmaisu raideliikennettä uhkaava tai uhkaan vaikuttava muu tapahtuma voidaan ymmärtää hyvin moninaisesti. Pykälän toimivaltuuden laajuudesta huolimatta kyseessä voi hyvinkin olla verkko- ja tietojärjestelmien turvallisuuden näkökulmasta niin sanottu paperitiikeri. Esimerkiksi palvelunestohyökkäykset ja kiristyshaittaohjelmahyökkäykset eivät kunnioita valtioiden rajoja ja tapahtuvat usein anonymiteetin suojista. Tällöin Liikenne- ja viestintäviraston Suomen lainsäädännön puitteissa tekemässä määräyksellä tuskin on merkittävää vaikutusta tietoturvahyökkäyksen jatkumiseen. Tulevaisuutta ennakoiden toimivaltuuden mahdollinen käyttötilanne voisi syntyä rautatieliikenteen automaation tason

noustessa, mikäli havaitaan riittämättömästi hallittu tietoturvariski. Tällöin säännös mahdollistaisi tietyn automaatiotason käytön rajoittamisen ja pakottaisi toimimaan matalammalla automaation tasolla, kunnes riski on asianmukaisesti hallinnassa.

Raideliikenteen toimintavaihtoehtojen erityistapauksena on raideliikennelain 173 §:n mukainen toiminta häiriötilanteessa. Kysymys ei ole Liikenne- ja viestintäviraston päätettävissä olevasta asiasta, vaan kyseessä on rataverkon haltijoiden velvollisuus sekä oikeus. Pykälän ensimmäisen momentin mukaan, ”[j]os raideliikenteessä esiintyy teknisistä ongelmista tai onnettomuudesta johtuvia häiriöitä, rataverkon haltijan on toteutettava kaikki tarvittavat toimenpiteet tilanteen palauttamiseksi ennalleen.” Pykälän sanamuodon mukainen soveltaminen ei siis ole rajattu koskemaan tietynlaisia häiriöitä vaan soveltamisalan voi katsoa kattavan myös verkko- ja tietojärjestelmien turvallisuuteen liittyvät häiriöt. Pykälän toisen momentin jälkimmäisen virkkeen mukaan ”[r]ataverkon haltija voi vaatia rautatieliikenteen harjoittajia antamaan sen käyttöön resurssit, joita se pitää tarpeellisena tilanteen palauttamiseksi ennalleen mahdollisimman nopeasti. – –.” Pykälän laatimisen taustalla on mahdollisesti ajatus hyödyntää rautatieliikenteenharjoittajien vetureita, vaunuja tai muuta olemassa olevaa liikkuvaa kalustoa. Pykälän sanamuoto ei kuitenkaan rajaa minkälaisista resursseista on kysymys. Tällöin esimerkiksi Väylävirasto rataverkon haltijana voisi vaatia VR-Yhtymä Oy:ltä tietoturvaresursseja käyttöönsä häiriön ratkaisemiseksi. Erityisen mielenkiintoinen pykälän soveltamistilanne syntyisi, mikäli Liikenne- ja viestintävirasto velvoittaisi Väyläviraston korjaamaan havaitun tietoturvapoikkeaman ja edelleen Väylävirasto vaatisi VR Yhtymä Oy:ltä resursseja häiriön poistamiseen.

Vesiliikenteessä VTS-palveluiden ja satamien osalta on yhtenevästi säädetty, että Liikenne- ja viestintäviraston on arvioitava toimijan tietoturvariskeinhallinnan vaikutuksia merenkulun turvallisuuteen, ryhdyttävä tarvittaessa korjaaviin toimenpiteisiin riskin poistamiseksi sekä tarvittaessa tehostettava velvoitetta uhkasakolla (Alusliikennepalvelulaki 28.4 § ja Turvatoimilaki 7 e.2 §). Hallituksen esityksessä tarkennetaan, että korjaavat toimenpiteiden kohteena olisi merkittävän riskin poistaminen ja merkittävällä riskillä tarkoitettaisiin samaa kuin merkittävän tietoturvahäiriön ilmoituskynnystä. (HE 192/2017 vp, s. 73-74) Lain sanamuodosta ja esitöistä ei tarkemmin ilmene korjaavien toimenpiteiden keinovalikoimaa, kuten tuleeko Liikenne- ja viestintäviraston poistaa merenkulun turvallisuuteen vaikuttava tietoturvariski antamalla tarkempia ohjeita, voiko riskin poistaa teetättämällä eli hyödyntämällä ulkopuolisia asiantuntijoita vai voiko virasto velvoittaa uhkasakon uhalla toimijan itsensä korjaamaan tilanteen. Myös käsitteellisesti pykälässä ilmaistu tavoite riskin poistamisesta on haastava, koska harvemmin riskiä on ylipäänsä mahdollista tai resurssien kohdentamisen näkökulmasta tarkoituksenmukaista kokonaan poistaa ja tyypillisempää on vähentää riskin todennäköisyyttä hyväksyttävälle tasolle. Alusliikennepalvelulaissa Liikenne- ja viestintävirastolle ei ole VTS-palveluihin liittyen säädetty muita toimintavaihtoehtoja. Sen sijaan satamien osalta tilanne on käytettävissä olevien toimintavaihtojen näkökulmasta suotuisampi. Mikäli satamanpitäjä ei

noudata turvatoimilain mukaisia säännöksiä, verkko- ja tietojärjestelmien turvallisuuden riskienhallintavelvollisuus mukaan lukien, Liikenne- ja viestintävirastolla on oikeus antaa ohjeita ja määräyksiä puutteiden ja epäkohtien korjaamiseksi, asettaa korjaustoimenpiteille määräaika sekä keskeyttää työt satamassa, kunnes epäkohdat on korjattu (Turvatoimilaki 19.1 §). Turvatoimilain 19 §:n toimintavaihtoehdot voi tulkita osittain päällekkäiseksi edellä mainittujen korjaaviin toimenpiteisiin ryhtymisen kanssa, jolloin tilanteesta riippuen määräyksen noudattamista voi tehostaa uhkasakolla tai uhkalla keskeyttää toiminta satamassa.

Tieliikenteessä Liikenne- ja viestintäviraston toimintavaihtoehdot ovat samat riippumatta siitä, onko kyseessä liikenteen ohjaus- ja hallintapalvelujen tarjoaja vai älykkään liikennejärjestelmän ylläpitäjä. Liikenteen palveluista annetun lain mukaan virastolla on verkko- ja tietojärjestelmien turvallisuuteen liittyviä velvoitteita rikottaessa oikeus velvoittaa toimija korjaamaan virheensä tai laiminlyöntinsä, tehostaa velvoitetta uhkasakolla, uhata keskeyttää toiminta tai teetättää tekemättömät toimenpiteet toimijan kustannuksella (Laki liikenteen palveluista 255.1 §). Hallituksen esityksen mukaan momentti vastaisi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain (617/2009) 45 §:ää. (HE 161/2016 vp, s. 166) Kyseisen pykälän yksityiskohtaisia perusteluita koskevassa hallituksen esityksen kohdassa tarkennetaan, että uhkasakko ja teetättämisuhka ovat ensisijaisia suhteessa toiminnan osan tai koko toiminnan keskeyttämiseen. (HE 36/2009 vp, s. 79)

Tietoturvahäiriöstä tiedottamisesta on säädetty kaikissa sektorikohtaisissa laeissa lähes yhtenäisesti: ”Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Liikenne- ja viestintävirasto voi velvoittaa palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.” (Raideliikennelaki 169.3 §, Alusliikennepalvelulaki 18 a.2 §, Turvatoimilaki 7 f.2 §, Laki liikenteen palveluista 161.3 §)[15] Tiedottamisen perustilanteena on, että keskeisen palvelun tarjoaja on ilmoittanut merkittävästä häiriöstä Liikenne- ja viestintävirastolle, jonka jälkeen kohdennetun tai rajoittamattoman tiedottamisen tarpeellisuutta arvioidaan yleisen edun näkökulmasta. Kuitenkin tiedottaminen on mahdollista myös silloin, kun keskeisen palvelun tarjoaja tietoisesti tai tiedostamatta ei ilmoita merkittävästä häiriöstä viranomaiselle. Tällöin viranomainen merkittävästä häiriöstä tiedon saatuaan voi selvittää onko kyseessä ilmoituskynnyksen ylittävästä tietoturvahäiriöstä ja velvoittaa palvelun tarjoajan itse tiedottamaan asiasta tai kuulla palveluntarjoajaa ja mahdollisesti tiedottaa itse häiriöstä. Tiedottamisen edellytyksenä on, että häiriöstä ilmoittaminen olisi yleisen edun mukaista. Hallituksen esityksessä ei tarkenneta kuinka yleinen etu tässä yhteydessä tulisi määritellä, mutta NIS-direktiivin 14(6) artiklan mukaan yksittäisistä poikkeamista tiedottamisen tarkoituksena olisi poikkeaman estäminen tai käynnissä olevan poikkeaman käsitteleminen. Direktiivin johdantokappale 59:n mukaan

[15] Laki liikenteen palveluista 140.3 §:ssä häiriön sijasta käytetään käsitettä poikkeama. Käsitteellisesti poikkeaman tulisi katsoa tarkoittavan samaa kuin häiriö, koska saman pykälän kahdessa muussa momentissa käytetään poikkeaman sijaan käsitettä häiriö.

yleisölle tiedottamisessa tulisi punnita keskenään yleistä etua saada tietoa uhista sekä tiedottamisesta aiheutuvia vahinkoja häiriöstä ilmoittaneen toimijan maineelle ja taloudelle. Johdantokappaleen mukaan viranomaisten tulisi erityisesti pidättäytyä tiedottamasta yksittäisiä tuotteita koskevista tietoturvahaavoittuvuuksista ennen kuin turvallisuuspäivitys haavoittuvuuden korjaamiseksi on julkaistu. Edellä esitetty huomioiden yleistä etua tulisi arvioida erityisesti siitä näkökulmasta, että pystytäänkö tiedottamisella estämään tietoturvallisuuteen liittyvien lisävahinkojen syntyminen taikka rajoittamaan tai lieventämään jo syntyneitä häiriöitä.

Liikenne- ja viestintäviraston käytettävissä olevien toimintavaihtoehtojen käsittelemisen jälkeen kappaleen lopuksi vielä arvioidaan, että vastaavatko käytettävissä olevat toimintavaihtoehdot NIS-direktiivin vähimmäisvaatimuksia. NIS-direktiivissä toimintavaihtoehdoista on säädetty artikloissa 15 ja 21. NIS-direktiivin artikla 15(3) mukaan toimivaltainen viranomainen voisi antaa sitovia ohjeita havaittujen puutteiden korjaamiseksi, mutta direktiivin sanamuotoa ei ole kirjoitettu jäsenvaltioita velvoittavaan muotoon. NIS-direktiivin johdantokappaleessa 61 tarkennetaan, että ”viranomaisilla olisi oltava tarvittavat keinot suorittaa tehtävänsä, mukaan lukien toimivalta saada riittävät tiedot arvioidakseen verkko- ja tietojärjestelmien turvallisuuden tason”. Vaikka johdantokappale tarkentaa toimivaltuuksien toivottua vähimmäistasoa, johdantokappaleen kirjaus ei muuta 15 artiklaa jäsenvaltioita velvoittavaksi. Seuraamuksista sen sijaan on säädetty jäsenvaltioita velvoittavassa muodossa. NIS-direktiivin 21 artiklan mukaan:

> ”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. – –.”

Artiklan kohta seuraamusten tehokkuudesta, oikeasuhtaisuudesta ja varoittavuudesta mukailee EU:n tietosuoja-asetuksen samankaltaista artiklaa sanktioista. Kuitenkin siinä missä tietosuoja-asetuksessa puhutaan hallinnollisista sakoista (administrative fines), NIS-direktiivissä kysymys on sääntöjen rikkomiseen sovellettavista seuraamuksista (penalties). Tietosuoja-asetuksesta eriävä sanamuoto mahdollistaa hieman laajemman kansallisen liikkumisvaran direktiivin täytäntöönpanossa seuraamusten muodon ja laadun osalta. Ainoastaan raideliikenteessä on käytettävissä suullinen tai kirjallinen huomautus sekä kirjallinen varoitus seuraamuksena verkko- ja tietojärjestelmien turvavelvoitteiden rikkomisesta. Näidenkin seuraamusten osalta voidaan aiheellisesti kyseenalaistaa, voidaanko niitä pitää tehokkaina tai varoittavina (dissuasive, avskräckande) ilman taloudellisen sanktion tai päätöksentekijöihin kohdistuvan muun seuraamuksen uhkaa. Lisäksi raide-, tie- ja vesiliikenteessä on mahdollisuus asettaa viranomaisen velvoitteen noudattamisen tehosteeksi uhkasakkolain mukainen uhkasakko. Uhkasakkoa ei kuitenkaan voi käyttää jälkikäteisenä seuraamuksena verkko- ja tietojärjestelmien riskienhallinnan laiminlyömisestä tai ilmoitusvelvollisuuden noudattamatta jättämisestä, vaan se soveltuu parhaiten havaittujen

puutteiden korjausvelvoitteiden tehostamiseen. Edellä esitetyn perusteella vaikuttaisi siltä, että NIS-direktiivin 21 artiklaa ei ole käsiteltyjen liikennöintimuotojen osalta Suomessa täysin saatettu osaksi kansallista lainsäädäntöä.

Yhteenvetona kappaleesta voi todeta, että raideliikenteessä käytettävissä on selkeästi laajin toimintavaihtoehtojen valikoima: Huomautus, varoitus, yksityiskohtainen määräys tai velvoite, uhkasakko, toimenpiteen teetättäminen, raideliikenteen keskeyttäminen, raideliikennettä uhkaavan tapahtuman tai toimenpiteen rajoittaminen. Lisäksi erityistapauksena Väylävirastolla rataverkon haltijana on verkko- ja tietojärjestelmien turvallisuushäiriöiden tilanteessa oikeus vaatia rautatieliikenteenharjoittajilta resursseja tilanteesta palautumiseksi. Tieliikenteen toimintavaihtoehdot ovat suppeammat koostuen velvoitteista korjata virheet, uhkasakosta velvoitteen tehosteeksi, toiminnan keskeyttämisuhka sekä toimenpiteiden teetättäminen. Satamien kohdalla käytettävissä oleva keinovalikoima vastaa lähes tieliikennettä, mutta teetättämistä ei ole nimenomaisesti vaihtoehtona laissa säädetty. Vähiten toimintavaihtoehtoja on käytettävissä vesiliikenteessä VTS-palveluiden kohdalla, jonka osalta ei voitane puhua toimintavaihtoehtojen valikoimasta, koska ainoa toimintavaihto on ryhtyä korjaaviin toimenpiteisiin ja tarvittaessa tehostaa velvoitetta uhkasakolla. Lisäksi kaikissa liikennemuodoissa on tietyin edellytyksin mahdollista velvoittaa keskeisen palvelun tarjoaja tiedottamaan häiriöstä tai viranomainen voi tiedottaa häiriöstä itse. Huomioiden että kaikissa liikennöintimuodoissa on kyse samankaltaisen verkko- ja tietojärjestelmien turvallisuusvelvoitteiden noudattamisen valvonnasta, voidaan pitää yllättävänä kuinka suuresti käytettävissä olevat toimintavaihtoehdot vaihtelevat liikennöintimuotojen välillä. Sen lisäksi että käytettävissä olevat toimintavaihtoehdot vaihtelevat suuresti, ne eivät myöskään vaikuta täyttävän sitä vähimmäistasoa, jota NIS-direktiivi jäsenvaltioilta edellyttää. Direktiivin mukaan jäsenvaltioiden on säädettävä direktiivin nojalla annettujen kansallisten säännösten rikkomiseen sovellettavista seuraamuksista. Ainoastaan raideliikenteessä seuraamuksista on säädetty, tosin seuraamukset rajoittuvat suullisten ja kirjallisten huomautusten sekä kirjallisten varoitusten antamiseen.

2.3.3 Määräystoimivalta

Kappaleessa selvitetään, minkälaista määräystoimivaltaa Liikenne- ja viestintävirastolle on säädetty, onko sitä hyödynnetty ja kuinka sitä mahdollisesti voisi hyödyntää tässä tutkimuksessa tunnistettujen sääntelyn ongelmakohtien selkeyttämiseksi. Tässä yhteydessä määräystoimivallalla tarkoitetaan viranomaiselle laissa säädettyä toimivaltuutta antaa lakeja ja asetuksia tarkentavia yleisiä määräyksiä, jotka julkaistaan viranomaisten määräyskokoelmassa ja ohjaavat tyypillisesti yksittäistä toimijaa laajempaa toimijaryhmää. Alakappaleessa käsiteltävä määräystoimivalta eroaa siten edellisessä alakappaleessa toimintavaihtoehtojen yhteydessä käsitellyistä ohjeista, määräyksistä ja velvoitteista, jotka ovat yksittäistä toimijaa koskevia hallintopäätöksiä.

Liikenne- ja viestintävirastolle on annettu määräystoimivaltaa sektorikohtaisessa lainsäädännössä. Raide- ja vesiliikenteen sekä tieliikenteessä älykkäiden liikennejärjestelmien kohdalla Liikenne- ja viestintäviraston määräystoimivalta

on samansisältöinen, mutta tieliikenteen liikenteenohjauspalveluiden osalta se on suppeampi. Raideliikennelain 169.5 §:n, alusliikennepalvelulain 18 a.4 §:n, turvatoimilain 7 f.4 §:n ja liikenteen palveluista annetun lain 161.5 §:n mukaan Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä siitä, milloin viestintäverkkoihin ja tietojärjestelmiin kohdistuva tietoturvallisuuteen liittyvä häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta. Toisin sanoen virastolle on annettu toimivalta antaa määräyksiä siitä, milloin viestintäverkkoihin tai tietojärjestelmiin kohdistuva häiriötä on pidettävä merkittävänä. Häiriön merkittävyyden määrittämistä koskeva määräystoimivaltuus on tärkeä edellä ilmoitusvelvollisuutta koskevassa kappaleessa käsitellyn ilmoitusvelvollisuuden kynnyksen tai vähimmäistason määrittelemiseksi. Ilmoituksen sisältöä, muotoa ja toimittamista koskeva määräystoimivalta mahdollistaa hyvin täsmällisen sääntelyn ilmoitusten yksityiskohdista. Kuitenkin sanamuodon perusteella määräystoimivalta ei ulotu ilmoitusten lukumäärän sääntelyyn eli ilmoitusvelvollisuutta koskevassa kappaleessa esitetty mahdollisuutta ennakkoilmoituksen, väli-ilmoituksen ja loppuraportin toimittamisesta ei määräystoimivallan käyttämisen perusteella voitaisi vaatia. Lisäksi määräystoimivalta ei yksiselitteisesti ulotu ilmoituksen aikarajoista määräämiseen. Kuitenkin olisi mahdollista puoltaa tulkintavaihtoehtoa, että määräystoimivalta ”ilmoituksen toimittamisesta” käsittäisi ilmoituksen välitysmuodon ja vastaanottajan määrittämisen lisäksi toimivallan määrätä ilmoituksen toimittamisen aikarajoista eli esimerkiksi, milloin ”viipymättä tehtävä ilmoitus” on viimeistään toimitettava.

Liikenne- ja viestintäviraston määräystoimivalta tieliikenteen ohjaus- ja hallintapalveluiden osalta muodostaa poikkeuksen muista käsitellyistä liikennöintimuodoista. Tieliikenteen ohjaus- ja hallintapalveluiden osalta virastolla on kuten muissakin liikennöintimuodoissa määräystoimivalta tarkentaa ilmoituksen sisältöä, muotoa ja toimittamistapaa, mutta virastolle ei ole annettu määräystoimivaltaa tarkentaa, milloin tietoturvahäiriötä on pidettävä merkittävänä (Laki liikenteen palveluista 140.2 §). On mahdollista, että lainsäätäjällä on tieliikenteen ohjaus- ja hallintapalveluiden kohdalla tapahtunut huolimattomuusvirhe, jonka seurauksena määräystoimivalta on jäänyt muita liikennöintimuotoja suppeammaksi. Tätä vaihtoehtoa tukevat ainakin kolme seikkaa. Ensinnäkin hallituksen esityksen yksityiskohtaisissa perusteluissa ei kerrota, miksi määräystoimivalta on säädetty suppeammaksi eikä asiaa muutoinkaan ole perusteltu. (HE 34/2018 vp, s. 86) Toiseksi merkittävän häiriön tarkentamista koskeva määräystoimialta on annettu Liikenne- ja viestintävirastolle kaikissa muissa liikennöintimuodoissa. Kolmanneksi Energiavirastolle sekä Maa- ja metsätalousministeriölle on omissa verkko- ja tietojärjestelmien turvallisuuden valvontatehtävissä säädetty häiriön merkittävyyttä koskeva määräystoimivalta. Toisin sanoen määräystoimivaltaa ei todennäköisesti ole tietoisesti säädetty suppeammaksi, vaan se on tiedostamatta säädetty muita kapeammaksi.

Liikenne- ja viestintävirasto ei ole hyödyntänyt määräystoimivaltaansa verkko- ja tietojärjestelmien turvallisuussääntelyn osalta, joskin valmiussuunnittelun näkökulmasta raideliikenteessä on sivuttu kyberturvallisuusriskienhallin-

taa Liikenne- ja viestintäviraston määräyksessä ”Valmiussuunnittelun järjestäminen liikennejärjestelmässä”. Määräystä ei sovelleta vesiliikenteen toimijoihin eikä tieliikenteen liikenteenohjaus- ja hallintapalveluiden tarjoajaan. Määräyksestä ei selkeästi ilmene, sovelletaanko sitä älykkäiden liikennejärjestelmien ylläpitäjiin. (Traficom, 2020c)

Tässä tutkimuksessa esille tulleiden havaintojen perusteella Liikenne- ja viestintäviraston voisi olla hyödyllistä määrätä, mitä merkittävällä tietoturvahäiriöllä tarkoitetaan ja minkälaiset aikarajat ilmoittamista koskevat. Määräyksessä voisi esimerkiksi tarkentaa, että häiriötä olisi pidettävä merkittävänä, kun häiriö tosiasiallisesti ja merkittävästi vaikuttaa toimijan riskienhallintavelvollisuuden kohteena oleviin viestintäverkkoihin ja tietojärjestelmiin ja voisi vaikuttaa kyseisen liikkumismuodon turvallisuuteen tai tosiasiallisesti merkittävästi vaikuttaa palvelun tarjoamisen jatkuvuuteen. Liikkumismuodon turvallisuuden mahdollinen vaarantuminen olisi riittävää eikä konkreettista vaarantumista vaadittaisi, koska vaaran konkretisoitumiseen vaikuttavat myös häiriön ulkopuoliset seikat sekä sattuma. Vaikutus palvelutason jatkuvuuteen tulisi ymmärtää palvelun saatavuuden tai laadun alentumisena normaalitasosta ajallisesti, alueellisesti tai käyttäjäryhmän näkökulmasta. Ilmoitus tulisi tehdä viipymättä. Ilmaus viipymättä tulisi ymmärtää niin, että ilmoitus on tehtävä heti kun toimija itse on merkittävästä häiriöstä tietoinen tai heti kun merkittävä häiriö on tapahtunut. Ilmoitus tulisi tehdä, kun häiriö on syntynyt, mutta toimijan ei tarvitse olla varma, että häiriö johtuu tietoturvallisuuden häiriötilasta. Riittävää olisi, että toimijalla on syytä epäillä, että häiriön juurisyynä on osittain tai kokonaan tietoturvahäiriö. Määräyksessä olisi syytä myös tuoda esille, että lakisääteisen ilmoitusvelvollisuuden lisäksi toimijat voivat myös vapaaehtoisesti ilmoittaa kaikista muista tietoturvahäiriöistä.

3 YHTEENVETO JA JOHTOPÄÄTÖKSET

Tutkielman tekemisen motiivina oli olettama, että voimassa oleva viestintäverkko- ja tietojärjestelmien turvallisuussääntely ei toimi ja yhtenä ongelman selittävänä tekijänä olisi tiedon puute sääntelyn sisällöstä eli muun muassa siitä, ketä sääntely koskee, mitä sääntely vaatii ja kuinka vaatimusten noudattamista valvotaan. Tämän olettaman myötä tutkielman tutkimuskysymykseksi muodostui, kuinka tutkimuksen keinoin voimassa olevaa NIS-sääntelyä voidaan systematisoida ja tulkita. Tutkimuskysymykseen vastaamista lähestyttiin analyyttisesti pilkkomalla kysymys pienempiin osatekijöihin, jotka selvittämällä pystyttiin vastaamaan pääkysymykseen.

Ensimmäisenä alakysymyksenä selvitettiin, mihin toimijoihin viestintäverkko- ja tietojärjestelmien turvallisuussääntely kohdistuu raide-, vesi- ja tieliikenteessä sekä vastaako soveltamisala NIS-direktiivin vähimmäistasoa.

Suomen lainsäädännöstä ei löydy yhtä määritelmää sille, mitä yhteiskunnan keskeisten palveluiden tarjoajat ovat. Sen sijaan yhteiskunnan keskeiset toiminnot ovat kattavasti listattu Valtioneuvoston periaatepäätöksessä yhteiskunnan turvallisuusstrategiasta, mutta NIS-direktiivin kansallisessa täytäntöönpanossa liikennesektorilla näitä kaikkia ei pidetty yhteiskunnan keskeisten palveluiden tarjoajana. NIS-direktiivin täytäntöönpanoa koskevassa hallituksen esityksessä sekä direktiivissä esitetään kolmekohtainen määritelmä keskeisten palveluiden tarjoajan määrittämiseksi. Määritelmä edellyttää ensinnäkin, että toimija tarjoaa palvelua, joka on keskeinen yhteiskunnan ja/tai talouden kriittisten toimintojen ylläpitämiseksi. Toiseksi vaaditaan, että kyseisen palvelun tarjoaminen on riippuvainen verkko- ja tietojärjestelmistä. Kolmantena vaatimuksena on, että poikkeamalla olisi merkittäviä haitallisia vaikutuksia kyseisen palvelun tarjoamiseen. Määritelmän ensimmäisen edellytyksen soveltaminen käytännössä pohjautuu NIS-direktiivin liitteen toimialaluetteloon. Määritelmän toisen kohdan soveltamisessa on yksinkertaisesti kyse siitä, perustuuko järjestelmän toiminta tietoverkkoihin ja tietojärjestelmiin vai onko kyseessä esimerkiksi joukko metalliputkeen kiinnitettyjä vanhoja peltisiä liikennemerkkejä, joiden tienkäyttäjille esittämään informaatioon ei tietoverkkojen ja tietojärjestelmien kautta voida vaikuttaa. Määritelmän kolmas kohta on erittäin tulkinnanvarainen ja tulkinnan

avuksi tutkielmassa tunnistetuista kriteereistä huolimatta se käytännössä mahdollistaa hyvin laajan, viime kädessä poliittisen, tarkoituksenmukaisuusharkinnan kriteeriä sovellettaessa.

Raideliikenteen osalta suoraan laissa yhteiskunnan keskeisten palveluiden tarjoajiksi on nimetty valtion rataverkon haltija eli Väylävirasto sekä liikenneohjauspalveluiden tarjoaja eli Fintraffic Raide Oy. Nykytilanteessa yhteiskunnan keskeisenä palveluna ei pidetä esimerkiksi VR-Yhtymä Oy:n varsinaista junien hallinnointia ja kuljettamista, yksityisraiteita kuten esimerkiksi Suomen vientisatamien raiteita tai kaupunkiraideliikenteestä esimerkiksi pääkaupunkiseudun metroa. Raideliikenteen liikenteenohjauspalveluiden osittaisulkoistamisesta johtuen on aidosti tulkinnanvaraista, tulisiko VR-Yhtymä Oy:tä sekä Destia Rail Oy:tä pitää myös yhteiskunnan keskeisen palvelun tarjoajana siltä osin, kun ne vastaavat Fintrafficin ulkoistamien ratapihojen liikenteenohjauksesta. Tutkimuksessa päädyttiin puoltamaan tulkintaa, että sääntelyä sovellettaisiin myös näihin kahteen yhtiöön, mutta myös päinvastaiselle tulkintavaihtoehdolle löytyy perusteita. Rautatieyritysten ja esimerkiksi junien käytännön kuljettamisen osalta NIS-direktiivi ei ehdottomasti velvoita kansallisesti soveltamaan sääntelyä rautatieyrityksiin. Rautatieyritysten osalta kuitenkin havaittiin, että hallituksen esityksessä on puutteellisesti perusteltu, kuinka nykyiseen ratkaisuun on päädytty erityisesti merkittävän haitallisen vaikutuksen arvioinnin osalta. NIS-direktiivin viittaukset rautatiemarkkinadirektiivin vaikuttaisivat mahdollistavan myös kaupunkiraiteiden haltijoiden kuten Pääkaupunkiseudun kaupunkiliikenne Oy:n (entinen HKL) ja Tampereen Raitiotie Oy:n sisällyttämisen rataverkon haltijoina sääntelyn piiriin, mutta tällaista näkökulmaa ei kansallisesti ole arvioitu. Yksityisraiteiden haltijat eivät myöskään kuulu yhteiskunnan keskeisiin palveluihin, mutta erityisesti satamaraiteiden osalta niillä on erittäin tärkeä rooli yhteiskunnan logistiikkaketjuissa ja niiden sisällyttämistä sääntelyn piiriin tulisi tulevaisuudessa arvioida uudelleen.

Vesiliikenteessä verkko- ja tietojärjestelmien turvallisuusvelvoitteita sovelletaan Fintraffic Meriliikenteenohjaus Oy:n VTS- eli alusliikennepalveluun AIS-järjestelmään liittyvät palvelut mukaan lukien sekä Turun, Naantalin, Hamina-Kotkan ja Helsingin satamiin. Satamien osalta Suomessa merkille pantavaa on, että Suomen suurin tavaraliikennesatama Porvoon Kilpilahdessa sekä Ahvenanmaan satamat jäävät soveltamisalan ulkopuolelle. Tutkimuksessa havaittiin, että varustamot on jätetty Suomessa sääntelyn soveltamisalan ulkopuolelle, mutta ulkopuolelle jättämisen perustelut hallituksen esityksessä eivät vaikuta vastaavan direktiivin vaatimuksia ja toisaalta 2020-luvun pandemian esille nostamat huoltovarmuuskysymykset antavat aihetta arvioida varustamoiden asemaa uudestaan. Mikäli tulevaisuudessa Suomi vähemmän valikoiden soveltaisi EU:n sisävesiä koskevaa sääntelyä, tällöin myös ECDIS-järjestelmän elektronisten merikartta-aineistojen tuotantoprosessi voisi olla syytä sisällyttää NIS-direktiivin soveltamisalaan, mutta tämä edellyttäisi tarkempaa pohdintaa, kuinka soveltamisen valvonta järjestettäisiin Traficomin itsensä ollessa ECDIS-järjestelmän käyttämän kartta-aineiston tuottaja.

Tieliikenteessä verkko- ja tietojärjestelmien turvallisuusvelvoitteita sovelletaan tieliikenteen liikenteenohjauspalvelun tarjoajaan, joka tällä hetkellä on Fintraffic Tie Oy. Älykkäiden liikennejärjestelmien osalta Liikenne- ja viestintävirasto Traficomin nykyisestä soveltamiskäytännöstä poiketen sääntely vaikuttaisi koskevan myös Hätäkeskuslaitosta eCall-järjestelmän hätäpuheluiden vastaanottamisen osalta sekä niitä Suomen oikeudenkäytön piirissä olevia yksityisiä palveluntarjoajia, jotka tekevät enemmän kuin vain automaattisesti välittävät eCall-hätäpuheluita Suomen Hätäkeskuslaitokselle. Lisäksi soveltamisalaan tulisi nykyisestä soveltamiskäytännöstä poiketen sisältyä Väylävirasto Digiroad-palvelun ylläpitäjänä sekä Fintraffic Digitraffic-palvelun ylläpitäjänä. Fintrafficin osalta velvoitteiden täsmällinen kohdentaminen riippuu yrityksen organisaatiorakenteesta ja erityisesti siitä, toteutetaanko Digitraffic palvelu Fintraffic Tie Oy:n organisaatiossa vai onko kyseessä Liikenteenohjausyhtiö Fintraffic Oy:n konsernitason palvelu. Tieliikenteen osalta tutkimuksessa ei tunnistettu ristiriitaisuuksia tai poikkeavuutta Suomen lainsäädännön NIS-direktiivin vähimmäisvaatimusten kanssa.

Johtopäätöksenä kappaleesta ”Keskeisten palveluiden tarjoajat” voidaan todeta, että verkko- ja tietojärjestelmien turvallisuussääntelyn kohteena olevien keskeisten palveluntarjoajien selvittämisen yhteydessä tunnistettiin ja hyödynnettiin kolmivaiheista määritelmää. Tätä määritelmää on mahdollista kehittää edelleen ja hyödyntää lähivuosina, mikäli NIS2 direktiiviluonnos hyväksytään EU:ssa ja sääntelyn soveltamisala laajenee uusiin organisaatioihin. Raideliikenteen ja tieliikenteen älykkäiden liikennejärjestelmien osalta sääntelyn soveltamisalassa tehnyt havainnot vahvistavat raide- ja tieliikenteen kyberturvallisuutta järjestelmätasolla sekä todennäköisesti johtavat siihen, että Liikenne- ja viestintävirasto Traficomin on tarvetta kohdentaa verkko- ja tietojärjestelmien turvasääntelyn valvontaa uusiin toimijoihin. Lisäksi näiden sääntelyn piiriin kuuluvaksi tunnistettujen toimijoiden on syytä varmistua, että heidän riskienhallinta täyttää lainsäädännön vähimmäisvaatimukset. Vesiliikenteen osalta sääntelyn soveltamisalan tutkiminen toi esiin vahvoja perusteita, miksi erityisesti vesiliikenteen osalta verkko- ja tietojärjestelmien turvavelvoitteiden soveltamisalaa olisi tarvetta tarkastella uudelleen ja laajentaa pandemian jälkeisessä ajassa.

Toisena alakysymyksenä tutkimuksessa selvitettiin, mitä verkko- ja tietojärjestelmien turvallisuussääntelyn kohteena olevilta toimijoilta vaaditaan riskienhallintavelvollisuuden ja ilmoittamisvelvollisuuden näkökulmista. Riskienhallintavelvollisuuden sisältö pilkottiin pienemmiksi osakysymyksiksi: Minkä riskienhallinnasta tulee varmistua, mikä on riskienhallinnan vähimmäistaso, miten vähimmäistason saavuttamisesta tulee varmistua ja kuinka riskienhallinta tulisi dokumentoida. Ilmoittamisvelvollisuuden sisällön määrittämistä lähestyttiin tutkimalla, minkälaisista tietoturvahäiriöistä viranomaisille tulee ilmoittaa ja milloin ilmoitus tulee tehdä.

Tutkielmassa esitettiin, että riskienhallinnan kohteena olevat viestintäverkot ja tietojärjestelmiä voi pyrkiä tunnistamaan jatkuvuudenhallinnan, turvallisuuteen kohdistuvan riskien, niiden turvallisuuden näkökulmasta merkittävyy-

den sekä operatiivisen toiminnan käsitteiden kautta. Näistä jatkuvuudenhallinnan käsite nousi keskeisimmäksi, koska sitä pidettiin käsitteenä laajimpana. Yhteiskunnan keskeisten palveluiden tarjoajien riskienhallintavelvollisuuden kohteena olisivat kaikki palvelun tarjoajan käyttämät viestintäverkot ja tietojärjestelmät, jotka 1) ovat kyseisen palvelun tarjoamisen jatkuvuuden tai häiriötilanteiden hallinnan kannalta keskeisiä tai 2) ovat kyseisen liikkumismuodon turvallisuuden kannalta merkittäviä taikka 3) joihin kohdistuvat häiriöt voisivat aiheuttaa riskin kyseisen liikennöintimuodon turvallisuudelle (tie-, raide- ja meriliikenteen ohjaus, valtion rataverkon haltija ja satamat) ja meriliikenteenohjauksen tilanteessa lisäksi liittyvät liikenteenohjaamisen operatiiviseen toimintaan.

Riskienhallinnan vähimmäistasolla tarkoitetaan asianmukaisia organisatorisia ja teknisiä toimenpiteitä, joilla varmistetaan riskienhallinnan kohteena olevien viestintäverkkojen ja tietojärjestelmien kyky suojautua tietyllä varmuudella tietoja tai palvelun saatavuutta, aitoutta, eheyttä tai luottamuksellisuutta vaarantavilta tapahtumilta. Riskienhallinnan vähimmäistason asianmukaisuutta on mahdollista tulkita taloudellisten realiteettien näkökulmasta ainakin silloin, kun kyse ei ole ihmisten hengestä ja terveydestä. Vaikka asianmukaisuuden tulkinnalle on löydettävissä useita kriteereitä, käsite saa tarkemman sisältönsä vasta toimintaa valvovan tahon tapauskohtaisessa soveltamisratkaisussa. Riskienhallinnan teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan teknisen tietoturvallisuuden lisäksi ihmisiin ja prosesseihin liittyviä toimenpiteitä ilman, että tietyn teknologian soveltamista ehdottomasti vaadittaisiin. Teknisten ja organisatoristen toimenpiteiden tyhjentävää luetteloa ei ole mahdollista esittää, mutta vaadittavien toimenpiteiden määrää voidaan pitää hyvinkin laajana, kun käsitteille haetaan tulkinta-apua ja esimerkkejä NIS-direktiivin johdantokappaleiden, NIS-direktiivin digitaalisten palveluiden tarjoajien vähimmäisvelvollisuuksien, sähköisen viestinnän palveluista annetun lain sekä tietosuoja-asetuksen ja kansallisesti hyvin tunnetusta Vastaamo -tapauksesta sekä standardointiorganisaatioiden kannanotoista. Teknisten ja organisatoristen toimenpiteiden vähimmäistasoa ei ole sidottu tiettyyn mittaristoon tai standardiin, mutta ENISA:n ja Valtioneuvoston kannanotot huomioiden ISO 27000 sarja ja erityisesti ISO 27001 nimetään mahdolliseksi tavoitetasoksi. Riskienhallinnan tarkoituksena on tietyllä varmuudella suojautua ei-toivotuilta tapahtumilta. Suojaustoimenpiteiden varmuudelle ei sääntelyssä aseteta tiettyä vähimmäistasoa, mutta sen voidaan ymmärtää merkitsevän samaa kuin NIS-direktiivin ilmaus riskiin suhteutettu tai Ruotsin lainsäädännössä käytetty ilmaus riskiperustaisuus. Keskeisenä edellytyksenä tietyn varmuuden tai riskiperustaisuuden määrittämiselle on yhteiskunnan keskeisen palvelun tarjoajan oman riskianalyysin laatiminen turvallisuustoimenpiteiden mitoittamiseksi. Riskin määrittämisen vähimmäistasosta voidaan todeta, että tarkastelu ei rajoitu vain puhtaasti tietotekniikasta itsestään johtuviin tekijöihin, vaan riskiarvioissa edellytetään kaikkien uhkatekijöiden huomioimista, olivat ne sitten luonnon tai ihmisen aiheuttamia, onnettomuuksia tai tahallaan aiheutettuja (ns. all-hazard approach). Kaikkien uhkatekijöiden tunnistamiseksi toimijalta ei kuitenkaan vaadita rajattomia kykyjä vaan riittävää on kohtuullisesti

tunnistettavissa olevien tilanteiden ja tapahtumien huomiointi. Tiedon jakaminen on yksi NIS-direktiivin perustavista tarkoituksista, mikä merkitsee sitä, että aikaisemmin raportoitua poikkeamaa tai tunnistettua riskiä tulisi jatkossa aina pitää kohtuullisesti tunnistettavissa olevana. Riskienhallintavelvollisuuteen sisältyvän dokumentaatiovelvollisuuden vähimmäistasosta voidaan todeta, että dokumentaatio tulee olla todennettavassa muodossa ja vähimmäistason täyttämiseen ei riitä pelkkä turvallisuusohjeen ja turvallisuuspolitiikan kirjallinen dokumentointi vaan velvollisuus on laajempi. Kuitenkaan laajuuden vähimmäistasosta ei voi tehdä tarkempia johtopäätöksiä, vaan laajuus tulee suhteuttaa yhteiskunnan keskeisen palvelun merkittävyyteen ja hyväksyttävän jäännösriskin suuruuteen pitäen mielessä, että dokumentaation ensisijainen tarkoitus on edistää toimijan tietoista riskienhallintaa ja riskienhallintakeinojen oikeasuhtaista mitoittamista. Suomessa riskienhallintavelvoite vaikuttaisi olevan NIS-direktiivin sanamuodon vähimmäistasoa alempi siltä osin, kun uusinta tekniikkaa ei suoranaisesti vaadita huomioitavan osana riskienhallintaa. Kuitenkin tutkimuksessa esitetty pyrkimys systematisoida ja tulkita riskienhallintavelvoitteen sisältöä osoittaa riskienhallintavelvoitteen sisältämän merkittävän tulkinnanvaraisuuden. Tämän johdosta riskienhallintavelvoitteen sanamuodot ei myöskään estä tulkitsemasta uusimman tekniikan vaatimuksen olevan sisäänrakennettu osa riskienhallintaa.

Ilmoittamisvelvollisuuden sisällön määrittämistä lähestyttiin tutkimalla, minkälaisista tietoturvahäiriöistä viranomaisille tulee ilmoittaa ja milloin ilmoitus tulee tehdä.

Yhteiskunnan keskeisten palveluiden tarjoajien on ilmoitettava merkittävistä tietoturvallisuuteen liittyvästä häiriöstä. Tutkimuksessa esitettiin, että häiriön merkittävyyttä arvioitaisiin sekä sen mahdollisten turvallisuusvaikutusten että sen tosiasiallisten jatkuvuuteen liittyvien vaikutusten kautta. Ilmoitus tietoturvahäiriöstä on tehtävä viipymättä, mutta tiettyä tuntirajaa käsitteelle ei säänte lystä ilmene. Kuitenkin yhteiskunnan keskeisen palvelun tarjoajan tulisi olla kohtuullisella todennäköisyydellä itse tietoinen häiriön olemassaolosta ja tapahtuman todentamiselle tulisi varata lyhyt hetki aikaa ennen kuin voitaisiin sanoa, että ilmoitusta ei ole tehty viipymättä. Ilmoitusvelvollisuuden kokonaisuus tutkimuksessa tiivistetään seuraavasti. Toimijoiden on ilmoitettava viipymättä eli ilman aiheetonta viivytystä mistä tahansa tapahtumasta, joka tosiasiallisesti ja merkittävästi vaikuttaa toimijan riskienhallintavelvollisuuden kohteena oleviin viestintäverkkoihin ja tietojärjestelmiin ja voisi vaikuttaa kyseisen liikkumismuodon turvallisuuteen tai tosiasiallisesti merkittävästi vaikuttaa palvelun tarjoamisen jatkuvuuteen.

Johtopäätöksenä kappaleesta ”Keskeisten palveluiden tarjoajien velvollisuudet” voidaan todeta, että verkko- ja tietojärjestelmien riskienhallinnan kohteelle tunnistettiin kolmen vaihtoehtoisen kriteerin määritelmä. Tätä määritelmää hyödyntämällä sekä keskeisen palvelun tarjoaja että valvova viranomainen voi tunnistaa, minkä tietoturvallisuudesta pitäisi varmistua. Riskienhallinnan vähimmäistason määrittämisen osalta tutkielmassa saavutettiin niin sanottu ne-

gatiivinen havainto eli tarkkarajaista vähimmäistasoa sääntelystä löydy ja toistaiseksi vähimmäistaso muotoutuu valvovan viranomaisen tulkintakannanottojen kautta. Tämä negatiivinen havainto myös kannustaa tutkimaan, voisiko riskienhallinnan vähimmäistason muotoilla jonkin muun tieteenalan kuin oikeustieteen keinoin. Merkittävistä tietoturvahäiriöistä ilmoittamiseksi tutkielmassa luotiin määritelmä, joka selventää ilmoitusvelvollisuuden sisältöä. Yhteisen määritelmän hyödyntäminen tietoturvahäiriöistä ilmoittamiseksi on tärkeää toimijoiden yhdenvertaisen kohtelun varmistamiseksi sekä valvovan viranomaisen resurssien kohdentamiseksi.

Kolmantena alakysymyksenä selvitettiin, minkälaisia valvontavelvollisuuksia Liikenne- ja viestintävirastolle on säädetty viestintäverkko- ja tietojärjestelmien turvallisuussääntelyyn liittyen, minkälaisia toimivaltuuksia valvonnan toteuttamiseksi on olemassa, mitä toimintavaihtoehtoja viranomaisella on havaittujen puutteiden korjaamiseksi tai häiriöihin reagoimiseksi sekä minkälaista sääntelyn sisältöä selkeyttävää määräystoimivaltaa Liikenne- ja viestintävirastolle on annettu.

Raideliikennelaista selkeästi ilmenee viraston velvollisuus valvoa, että Väylävirasto rataverkon haltijana noudattaa verkko- ja tieturvallisuusvelvollisuuksia. Kuitenkin raideliikenteen liikenteenohjauspalveluiden osalta asia ei ole näin selkeä. Selvää on, että virastolla on liikenteenohjauspalveluihin kohdistuva valvontavelvollisuus siltä osin, kun verkko- ja tietojärjestelmien turvavelvoite kohdistuu radan ohjaus-, hallinta- ja merkinanto-, energia- tai infrastruktuuriosajärjestelmään. Verkko- ja tietojärjestelmien turvallisuuden valvontavelvollisuus on myös siltä osin, kun rautatieliikenteenharjoittaja huolehtii liikenteenohjauksesta Fintrafficin ulkoistaman liikenteenohjauksen osalta. Raideliikennelaissa Liikenne- ja viestintävirastolle ei ole kuitenkaan säädetty suoraa velvollisuutta valvoa, että Fintraffic Raide Oy noudattaa sille raideliikennelaissa säädettyjä verkko- ja tietojärjestelmien turvallisuuden hallinta ja ilmoittamisvelvollisuuksia. Liikenne- ja viestintävirastolla on kuitenkin välillinen velvoite valvoa raideliikenteen liikenteenohjauspalveluiden verkko- ja tietojärjestelmien turvallisuusvelvoitteita, koska Liikenne- ja viestintävirasto valvoo Väylävirastoa ja Väyläviraston tulee turvallisuusjohtamisjärjestelmällä osoittaa liikenteenohjauspalveluntarjoajan noudattavan verkko- ja tietojärjestelmien turvavelvoitteita. Liikenne- ja viestintäviraston suoran raideliikenteen liikenteenohjauspalveluihin kohdistuvan valvontavelvollisuuden puute on kuitenkin ongelmallinen, koska ilman lakiin perustuvaa valvontavelvollisuutta ei virasto voi hyödyntää sille säädettyjä valvontatehtävään sidottuja valvontatoimivaltuuksia. Vesi- ja tieliikenteessä viraston velvollisuus valvoa tutkimuksessa tunnistettuja keskeisten palveluiden tarjoajia ilmenee selkeästi sektorikohtaisesta lainsäädännöstä, joskin satamien kohdalla turva-arvioinnin voidaan katsoa ulottuvan perinteistä valvontaa pidemmälle kohti riskienhallinnan määrittelyvelvoitetta. Valvontavelvollisuuksien osalta vesi- ja tieliikennesektoreilla Suomen lainsäädäntö vaikuttaa olevan yhteensopiva NIS-direktiivin vähimmäisvaatimusten kanssa, mutta raideliikenteen osalta kysymys on tulkinnanvarainen. Tutkimuksessa päädyn puoltamaan tulkintaa, että raideliikenteen valvontavelvollisuus liikenteenohjauspalveluiden

osalta ei välttämättä täytä NIS-direktiivin vähimmäisvaatimusta siltä osin, kun kyse on jäsenvaltion velvollisuudesta varmistaa tarvittava toimivaltuus ja keinot arvioida verkko- ja tietojärjestelmien turvallisuussääntelyn noudattamista.

Varovaisesti yleistäen voi luonnehtia, että Liikenne- ja viestintäviraston toimivaltuudet ovat selkeästi laajimmat raideliikenteessä ja vähäisimmät vesiliikenteessä VTS-palveluiden osalta. Raideliikenteessä viraston toimivaltuudet kattavat pääsyn tiloihin ja laitteisiin ilman ennakkoilmoitusta, oikeuden hyödyntää ulkopuolista asiantuntijaa, oikeuden valvoa henkilöstöä sekä tiedonsaantioikeuden. Tieliikenteessä toimivaltuudet kattavat oikeuden päästä toimitiloihin, saada tarkastuksen kohteelta apua, hyödyntää ulkopuolista asiantuntijaa sekä oikeuden saada tietoa. Satamien kohdalla ainoa selkeä toimivaltuus on tiedonsaantioikeus, mutta turva-arvioinnin toteuttamisen voi ymmärtää luonnollisesti kattavan myös oikeuden päästä arvioitavaan kohteeseen ja havainnoida kaikkea toimintaa kohteessa. VTS-palveluiden osalta Liikenne- ja viestintävirastolle ei ole säädetty samankaltaisia varsinaisia valvontatoimivaltuuksia kuten muissa liikennöintimuodoissa, mutta VTS-palveluiden kohdalla toimivaltuutena on hyväksyä tai olla hyväksymättä VTS-palveluntarjoajan ylläpitämää toimintakäsikirjaa. VTS-palveluiden verkko- ja tietojärjestelmien turvallisuusvelvoitteiden valvontatoimivaltuuksien suppeus vaikuttaa olevan ristiriidassa NIS-direktiivin kanssa, koska jäsenvaltioiden tulisi varmistaa toimivaltaiselle viranomaiselle tarvittava tietojensaantioikeus verkko- ja tietojärjestelmien turvallisuuden arvioimiseksi, joka kattaa tiedonsaannin turvallisuusohjeista, turvallisuusohjeiden täytäntöönpanoa osoittavasta näytöstä sekä turvallisuustarkastuksien tuloksista ja tuloksia tukevasta näytöstä.

Arvioitaessa mitä toimintavaihtoehtoja viranomaisella on havaittujen puutteiden korjaamiseksi tai häiriöihin reagoimiseksi, voidaan todeta, että raideliikenteessä on käytettävissä selkeästi laajin toimintavaihtoehtojen valikoima: Huomautus, varoitus, yksityiskohtainen määräys tai velvoite, uhkasakko, toimenpiteen teetättäminen, raideliikenteen keskeyttäminen, raideliikennettä uhkaavan tapahtuman tai toimenpiteen rajoittaminen. Lisäksi erityistapauksena Väylävirastolla rataverkon haltijana on verkko- ja tietojärjestelmien turvallisuushäiriöiden tilanteessa oikeus vaatia rautatieliikenteenharjoittajilta resursseja tilanteesta palautumiseksi. Tieliikenteen toimintavaihtoehdot ovat suppeammat koostuen velvoitteista korjata virheet, uhkasakosta velvoitteen tehosteeksi, toiminnan keskeyttämisuhka sekä toimenpiteiden teetättäminen. Satamien kohdalla käytettävissä oleva keinovalikoima vastaa lähes tieliikennettä, mutta teetättämistä ei ole nimenomaisesti vaihtoehtona laissa säädetty. Vähiten toimintavaihtoehtoja on käytettävissä vesiliikenteessä VTS-palveluiden kohdalla, jonka osalta ei voitane puhua toimintavaihtoehtojen valikoimasta, koska ainoa toimintavaihto on ryhtyä korjaaviin toimenpiteisiin ja tarvittaessa tehostaa velvoitetta uhkasakolla. Lisäksi kaikissa liikennemuodoissa on tietyin edellytyksin mahdollista velvoittaa keskeisen palvelun tarjoaja tiedottamaan häiriöstä tai viranomainen voi tiedottaa häiriöstä itse. Huomioiden että kaikissa liikennöintimuodoissa on kyse samankaltaisen verkko- ja tietojärjestelmien turvallisuusvelvoitteiden noudattamisen

valvonnasta, voidaan pitää yllättävänä kuinka suuresti käytettävissä olevat toimintavaihtoehdot vaihtelevat liikennöintimuotojen välillä. Sen lisäksi että käytettävissä olevat toimintavaihtoehdot vaihtelevat suuresti, ne eivät myöskään vaikuta täyttävän sitä vähimmäistasoa, jota NIS-direktiivi jäsenvaltioilta edellyttää. Direktiivin mukaan jäsenvaltioiden on säädettävä direktiivin nojalla annettujen kansallisten säännösten rikkomiseen sovellettavista seuraamuksista. Ainoastaan raideliikenteessä seuraamuksista on säädetty, tosin seuraamukset rajoittuvat suullisten ja kirjallisten huomautusten sekä kirjallisten varoitusten antamiseen.

Raide- ja vesiliikenteen sekä tieliikenteessä älykkäiden liikennejärjestelmien kohdalla Liikenne- ja viestintävirastolle on annettu toimivalta antaa tarkempia määräyksiä siitä, milloin viestintäverkkoihin ja tietojärjestelmiin kohdistuva tietoturvallisuuteen liittyvä häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta. Liikenne- ja viestintäviraston määräystoimivalta tieliikenteen ohjaus- ja hallintapalveluiden osalta muodostaa poikkeuksen muista käsitellyistä liikennöintimuodoista. Tieliikenteen ohjaus- ja hallintapalveluiden osalta virastolla on kuten muissakin liikennöintimuodoissa määräystoimivalta tarkentaa ilmoituksen sisältöä, muotoa ja toimittamistapaa, mutta virastolle ei ole annettu määräystoimivaltaa tarkentaa, milloin tietoturvahäiriötä on pidettävä merkittävänä.

Tutkimuksessa esille tulleiden havaintojen perusteella Liikenne- ja viestintäviraston voisi olla hyödyllistä määrätä, mitä merkittävällä tietoturvahäiriöllä tarkoitetaan ja minkälaiset aikarajat ilmoittamista koskevat. Määräyksessä voisi esimerkiksi tarkentaa, että häiriötä olisi pidettävä merkittävänä, kun häiriö tosiasiallisesti ja merkittävästi vaikuttaa toimijan riskienhallintavelvollisuuden kohteena oleviin viestintäverkkoihin ja tietojärjestelmiin ja voisi vaikuttaa kyseisen liikkumismuodon turvallisuuteen tai tosiasiallisesti merkittävästi vaikuttaa palvelun tarjoamisen jatkuvuuteen. Liikkumismuodon turvallisuuden mahdollinen vaarantuminen olisi riittävää eikä konkreettista vaarantumista vaadittaisi, koska vaaran konkretisoitumiseen vaikuttavat myös häiriön ulkopuoliset seikat sekä sattuma. Vaikutus palvelutason jatkuvuuteen tulisi ymmärtää palvelun saatavuuden tai laadun alentumisena normaalitasosta ajallisesti, alueellisesti tai käyttäjäryhmän näkökulmasta. Ilmoitus tulisi tehdä viipymättä. Ilmaus viipymättä tulisi ymmärtää niin, että ilmoitus on tehtävä heti kun toimija itse on merkittävästä häiriöstä tietoinen tai heti kun merkittävä häiriö on tapahtunut. Ilmoitus tulisi tehdä, kun häiriö on syntynyt, mutta toimijan ei tarvitse olla varma, että häiriö johtuu tietoturvallisuuden häiriötilasta. Riittävää olisi, että toimijalla on syytä epäillä, että häiriön juurisyynä on osittain tai kokonaan tietoturvahäiriö. Määräyksessä olisi syytä myös tuoda esille, että lakisääteisen ilmoitusvelvollisuuden lisäksi toimijat voivat myös vapaaehtoisesti ilmoittaa kaikista muista tietoturvahäiriöistä.

Johtopäätöksenä kappaleesta ”Liikenne- ja viestintäviraston toimivalta valvovana viranomaisena” voidaan todeta, että raideliikenteessä valvontavelvollisuuksien epäselvyys voi heikentää raideliikenteen kyberturvallisuutta, minkä lisäksi nykyinen asiantila ei välttämättä täytä NIS-direktiivin Suomelle asettamia

vähimmäisvaatimuksia. Koko liikennejärjestelmän näkökulmasta tarkasteltuna valvonnan tekemiseksi käytettävissä olevien valvontatoimivaltuuksien merkittävät eroavaisuudet eri liikennemuotojen välillä luovat liikenteen kyberturvallisuuden valvontaan tehottomuutta Liikenne- ja viestintäviraston sisällä, koska samoja valvontakeinoja ei voida käyttää kaikissa liikennemuodoissa. Tutkielman havainnot verkko- ja tietojärjestelmien turvallisuussääntelyn rikkomisen seuraamuksien puutteista merkitsevät, että mikäli lähivuosina NIS2 direktiivi tulisi saattaa Suomessa kansallisesti voimaan, seuraamusten tai sanktioiden sääntelyn laatiminen vaatii erityistä huomiota, koska nykyisestä sääntelystä seuraamuksia ei varsinaisesti löydy. Seuraamusten puute myös osaltaan merkitsee, että sääntelyn kohteena olevilla organisaatioilla ei välttämättä ole niin suuria kannustimia korjata riskienhallinnan puutteita ennen kuin valvova viranomainen tällaisia havaintoja löytää. Tutkielman havainnot kokonaisuutena myös luovat taustaselvityksen, jota olisi mahdollista hyödyntää, mikäli Liikenne- ja viestintävirasto Traficom antaisi määräyksen verkko- ja tietojärjestelmien turvasääntelyn noudattamisesta liikennejärjestelmässä. Lisäksi tutkielmassa esitetyt kannanotot voisivat toimia mahdollisen määräyksen luonnostelun perustana.

LÄHTEET

Kirjallisuus (kirjat, artikkelit)

Alhamo, L. (2021). Kone- ja tietoturvallisuus - Riskien arvioinnin suhteet ja laillinen viitekehys. Opinnäytetyö, Tampereen ammattikorkeakoulu.

Kolehmainen, A. (2015). Tutkimusongelma ja metodi lainopillisessa työssä. Teoksessa Miettinen, T. (toim.), *Oikeustieteellinen opinnäyte - artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta*, ss. 106-134, EDILEX Edita Publishing.

Markopoulou, D., Papakonstantinou, V. ja de Hert P (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer law & security review 35*. https://doi.org/10.1016/j.clsr.2019.06.007

Porcedda, M. (2018). Patching the patchwork: appraising the EU regulatory framework on cyber security breaches. *Computer Law & Security Review, Volume 34, Issue 5, 2018*. https://doi.org/10.1016/j.clsr.2018.04.009

Pöyhönen, J. (2020). Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa. Väitöskirja, Jyväskylän yliopisto.

Rantala, J. (2017). NIS-direktiivin kahdet kasvot - riskit ja riskienhallinta. Pro gradu -tutkielma, Jyväskylän yliopisto.

Schmitz-Berndt, S. & Schiffner, S. (2021). Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR. *International Review of Law, Computers & Technology, 35:2, p. 101-115*, DOI: 10.1080/13600869.2021.1885103

Siltala, R. (2003). Oikeustieteen tieteenteoria. *Suomalaisen lakimiesyhdistyksen julkaisuja. A sarja n:o 234,* Vammalan kirjapaino.

Soikkeli, M. (2021). Lainsäädäntö tieto- ja kyberturvallisuuden perustana - valtionhallinnon viranomaisen näkökulma. Pro gradu -tutkielma, Jyväskylän yliopisto.

Söderholm, A. (2018). Threats and Challenges around European Cyber Security Cooperation in the Context of the European Union Directive on Security of Network and Information Systems. Pro gradu -tutkielma, Jyväskylän yliopisto.

Talus, K. & Penttinen, S. (2015). Eurooppaoikeudelliset oikeuslähteet ja niiden tulkinta oikeustieteellistä opinnäytettä kirjoitettaessa. Teoksessa Miettinen, T. (toim.), *Oikeustieteellinen opinnäyte - artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta*, ss. 223-245, EDILEX Edita Publishing.

Virallislähteet

Suomi (muistiot, HE, ministeriön julkaisut, periaatepäätökset)

HE 262/2010 vp Hallituksen esitys Eduskunnalle rautatielaiksi.

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

HE 161/2016 vp Hallituksen esitys liikennekaareksi ja eräiksi siihen liittyviksi laeiksi.

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

HE 34/2018 vp Hallituksen esitys eduskunnalle laiksi Liikenneviraston liikenteenohjaus- ja hallintapalveluiden muuttamisesta osakeyhtiöksi ja eräiksi siihen liittyviksi laeiksi.

HE 105/2018 vp Hallituksen esitys eduskunnalle raideliikennelaiksi ja laiksi liikenteen palveluista annetun lain muuttamisesta.

HE 284/2018 vp. Hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi.

LVM (2017). Verkko- ja tietoturvadirektiivi. Kansallista täytäntöönpanoa tukevan työryhmän loppuraportti, Liikenne- ja viestintäministeriön julkaisuja 9/2017. http://urn.fi/URN:ISBN:978-952-243-505-7

LVM (2018). Muistio koskien valtioneuvoston asetusta yhteiskunnan toiminnan kannalta merkittävistä lentoasemista ja satamista 2.5.2018. Liikenne- ja viestintäministeriö. https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f805b1b33

LVM (2021). Perusmuistio. Komission tiedonanto/ NAIADES III: Tulevaisuudenkestävän eurooppalaisen sisävesiliikenteen tukeminen 17.9.2021. Liikenne- ja viestintäministeriö. https://www.eduskunta.fi/FI/vaski/Liiteasiakirja/Documents/EDK-2021-AK-389475.pdf

Miettinen, K., Miettinen, A., Hauta, J., Töyrylä, S., Reinimäki, S. (2021). Liikenteen automaation lainsäädäntö- ja avaintoimenpidesuunnitelma. Liikenne- ja viestintäministeriön julkaisuja 2021:28. http://urn.fi/URN:ISBN:978-952-243-726-6

Pylvänäinen, J., Lehtola, J., Toivakka, L., Westerling, J., Tervola, V., Tiilikainen, A., Brotherus, M., Ahtiainen, L., Kuismin, J. (2021). Kohti digitaalista ja älykästä rautatieliikennettä. Digirata-valmisteluvaiheen loppuraportti. Liikenne- ja viestintäministeriön julkaisuja 2021:17. http://urn.fi/URN:ISBN:978-952-243-596-5

Turvallisuuskomitea (2017). Yhteiskunnan turvallisuusstrategia 2017. Valtioneuvoston periaatepäätös. Turvallisuuskomitea,

Puolustusministeriö. https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf

Valtioneuvosto (2021). Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla. Valtioneuvosto 10.6.2021. https://valtioneuvosto.fi/delegate/file/90935.

Suomi lait, asetukset ja määräykset

Asetus ihmishengen turvallisuudesta merellä vuonna 1974 tehdyn kansainvälisen yleissopimuksenliitteeseen tehtyjen muutosten voimaansaattamisesta (Valtiosopimus 50/1998).

Alusliikennepalvelulaki 5.8.2005/623.

Laki eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta 11.6.2004/485.

Laki julkisen hallinnon tiedonhallinnasta 906/2019.

Laki liikenteen palveluista 24.5.2017/320.

Liikenne- ja viestintävirasto Traficom (2020). Valmiussuunnittelun järjestäminen liikennejärjestelmässä 15.5.2020. TRAFICOM/308489/03.04.04.00/2019.

Liikenteen turvallisuusvirasto (2012). Merenkulku ja vesiliikenne: Alusten navigointilaitteet ja -järjestelmät 22.11.2012. TRAFI/16915/03.04.01.00/2012.

Raideliikennelaki 28.12.2018/1302.

Suomen perustuslaki 731/1999.

Valtioneuvoston asetus yhteiskunnan toiminnan kannalta merkittävistä lentoasemista ja satamista 361/2018.

Valtioneuvoston asetus meriliikenteen tukemisesta 548/2020.

Viestintävirasto (2016a). Määräys hätäliikenteen teknisestä toteutuksesta ja varmistamisesta. Viestintävirasto 33 G/2016 M, 20.12.2016.

Viestintävirasto (2016b). Määräyksen 33 perustelut ja soveltaminen. Hätäliikenteen teknisestä toteutuksesta ja varmistamisesta. 20.12.2016. MPS 33.

Ruotsi lait

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digi-tala tjänster. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174

Euroopan unioni

Asetukset ja direktiivit

Euroopan parlamentin ja neuvoston asetus (EU) 2015/758, annettu 29 päivänä huhtikuuta 2015, hätänumeroon 112 perustuvan ajoneuvoon asennettavan

eCall-järjestelmän käyttöönottoa koskevista tyyppihyväksyntävaatimuksista ja direktiivin 2007/46/EY muuttamisesta.

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.

Euroopan parlamentin ja neuvoston asetus (EU) N:o 1315/2013, annettu 11 päivänä joulukuuta 2013 , unionin suuntaviivoista Euroopan laajuisen liikenneverkon kehittämiseksi ja päätöksen N:o 661/2010/EU kumoamisesta.

Euroopan parlamentin ja neuvoston asetus (EY) N:o 725/2004, annettu 31 päivänä maaliskuuta 2004, alusten ja satamarakenteiden turvatoimien parantamisesta.

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

Euroopan parlamentin ja neuvoston direktiivi 2002/59/EY, annettu 27 päivänä kesäkuuta 2002, alusliikennettä koskevan yhteisön seuranta- ja tietojärjestelmän perustamisesta sekä neuvoston asetuksen 93/75/ETY kumoamisesta.

Euroopan parlamentin ja neuvoston direktiivi 2005/44/EY, annettu 7 päivänä syyskuuta 2005, yhdenmukaistetuista jokitiedotuspalveluista (RIS) Euroopan yhteisön sisävesillä.

Euroopan parlamentin ja neuvoston direktiivi 2005/65/EY, annettu 26 päivänä lokakuuta 2005, satamien turvallisuuden parantamisesta.

Euroopan parlamentin ja neuvoston direktiivi 2009/140/EY, annettu 25 päivänä marraskuuta 2009, sähköisten viestintäverkkojen ja -palvelujen yhteisestä sääntelyjärjestelmästä annetun direktiivin 2002/21/EY, sähköisten viestintäverkkojen ja niiden liitännäistoimintojen käyttöoikeuksista ja yhteenliittämisestä annetun direktiivin 2002/19/EY sekä sähköisiä viestintäverkkoja ja -palveluja koskevista valtuutuksista annetun direktiivin 2002/20/EY muuttamisesta.

Euroopan parlamentin ja neuvoston direktiivi 2010/40/EU, annettu 7 päivänä heinäkuuta 2010, tieliikenteen älykkäiden liikennejärjestelmien käyttöönoton sekä tieliikenteen ja muiden liikennemuotojen rajapintojen puitteista.

Euroopan parlamentin ja neuvoston direktiivi 2012/34/EU, annettu 21 päivänä marraskuuta 2012, yhtenäisestä eurooppalaisesta rautatiealueesta.

Komission asetus (EY) N:o 414/2007, annettu 13 päivänä maaliskuuta 2007, yhdenmu-kaistetuista jokitiedotuspalveluista (RIS) Euroopan yhteisön sisävesillä annetun Euroopan parlamentin ja neuvoston direktiivin

2005/44/EY 5 artiklassa tarkoitetuista teknisistä ohjeis-ta jokitiedotuspalvelujen suunnittelua, täytäntöönpanoa ja käyttöä varten.

Komission delegoitu asetus (EU) 2015/962, annettu 18 päivänä joulukuuta 2014, Euroopan parlamentin ja neuvoston direktiivin 2010/40/EU täydentämisestä EU:n laajuisten tosiaikaisten liikennetietopalvelujen tarjoamisen osalta.

Komission täytäntöönpanoasetus (EU) 2018/1973, annettu 7 päivänä joulukuuta 2018, Euroopan parlamentin ja neuvoston direktiivissä 2005/44/EY tarkoitetuista sisävesiliikenteen elektronista merikarttajärjestelmää (sisävesien ECDIS-järjestelmä) koskevista teknisistä eritelmistä annetun täytäntöönpanoasetuksen (EU) N:o 909/2013 muuttamisesta.

Komission täytäntöönpanoasetus (EU) 2019/838, annettu 20 päivänä helmikuuta 2019, alusten paikannus- ja seurantajärjestelmiä koskevista teknisistä eritelmistä ja asetuksen (EY) N:o 415/2007 kumoamisesta.

Kansainväliset sopimukset

Sopimus ihmishengen turvallisuudesta merellä vuonna 1974 (SOLAS)

Muut lähteet (direktiiviehdotukset, EU:n virastojen ja työryhmien raportit)

Ehdotus euroopan parlamentin ja neuvoston direktiivi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta, Euroopan komissio, 16.12.2020.

Ehdotus euroopan parlamentin ja neuvoston direktiiviksi kriittisten toimijoiden häiriönsietokyvystä, Euroopan komissio 16.12.2020.

ENISA (2016). Gaps in NIS standardisation - Recommendations for improving NIS in EU standardisation policy v. 1.0, November 2016. European Union Agency For Network And Information Security. https://www.enisa.europa.eu/publications/gaps-eu-standardisation/@@download/fullReport

EUR-lex (2022, tammikuu). Menettely 2020/0359/COD, COM (2020) 823: Proposal for a directive of the european parliament and of the council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. Viimeksi vierailtu 6.2.2022. https://eur-lex.europa.eu/procedure/EN/2020_359

NIS Cooperation Group (2018a). Reference document on security measures for Operators of Essential Services. *NIS Cooperation Group publication* 01/2018. http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643

NIS Cooperation Group (2018b). Reference document on Incident Notification for Operators of Essential Services, Circumstances of notification. *NIS Cooperation Group publication 02/2018*. http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53644

NIS Cooperation Group (2018c). Identification of Operators of Essential Services, Reference document on modalities of the consultation process in cases with cross-border impact. *NIS Cooperation Group publication 07/2018.* http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53661

NIS Cooperation Group (2021). Annual Report NIS Directive Incidents 2020. *NIS Cooperation Group publication*, June 2021. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148, Council of the European Union, 26.11.2021

Tietosuojatyöryhmä WP29 (2018). Suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksesta ilmoittamisesta, WP250rev.01, annettu 3.10.2017, viimeksi tarkistettu ja hyväksytty 6.2.2018. https://ec.europa.eu/newsroom/article29/redirection/document/49827

Internetlähteet ja tiedotteet

DigitalEurope (2016). Transposition of the EU Network and Information Security (NIS) Directive. Brussels, 5.7.2016. https://www.digitaleurope.org/wp/wp-content/uploads/2019/01/DIGITALEUROPE%20Views%20on%20Transposition%20of%20the%20EU%20Network%20and%20Information%20Security%20(NIS)%20Directive.pdf

ETSI (2017). Technical Report CYBER; Implementation of the Network and Information Security (NIS) Directive, ETSI TR 103 456 V1.1.1 (2017-10), DTR/CYBER-0021.

ETSI (2018). Technical report Cyber; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls. ETSI TR 103 305-1 V3.1.1 (2018-09), RTR/CYBER-0034-1.

Fintraffic (2021, toukokuu 11). Fintraffic kilpailutti ratapihaliikenteenohjauspalvelut: VR-Yhtymä Oy ja Destia Rail Oy kumppaneiksi. Liikenteenohjausyhtiö Fintraffic Oy. Viimeksi vierailtu 6.2.2022. https://www.fintraffic.fi/fi/uutiset/fintraffic-kilpailutti-ratapihaliikenteenohjauspalvelut-vr-yhtyma-oy-ja-destia-rail-oy

Fintraffic (2022a). Fintraffic Tie lyhyesti. Fintraffic Tie Oy. Viimeksi vierailtu 16.2.2022. https://www.fintraffic.fi/fi/tie/fintraffic-tie-lyhyesti

Fintraffic (2022b). Liikennevaloetuusjärjestelmä HALI. Fintraffic Tie Oy. Viimeksi vierailtu 16.2.2022. https://www.fintraffic.fi/fi/tie/liikennevaloetuusjarjestelma-hali

Furuno. Furuno Finland Oy. Viimeksi vierailtu 9.2.2022. https://www.furuno.fi/fin/furuno_finland_oy/

Fintraffic (2022c). Digitraffic. Viimeksi vierailtu 20.2.2022. https://www.digitraffic.fi/

First.org (2019). Common Vulnerability Scoring System v.3.1: Specification document. Forum of Incident Response and Security Teams. Viimeksi vierailtu 20.2.2022. https://www.first.org/cvss/v3.1/specification-document#7-1-Base-Metrics-Equations

Ginindza, B (2021, July 23). Transnet 'cyber attack' causes logistics logjam from road to freight and ports. IOL.Viimeksi vierailtu 6.2.2022. https://www.iol.co.za/business-report/economy/transnet-cyber-attack-causes-logistics-logjam-from-road-to-freight-and-ports-56f6bd97-c5ef-4d65-90d6-c41d0fe290e2

Helsinki (2021). Tietoja HKL:stä. Helsigin kaupunki. Viimeksi vierailtu 28.12.2021. https://www.hel.fi/hkl/fi/tama-on-hkl/organisaatio/

HILMA (2020, elokuu 19). Ratapihaliikenteenohjauspalvelu. Julkisten hankintojen hankintailmoitukset. Viimeksi vierailtu 6.2.2022. https://www.hankintailmoitukset.fi/fi/public/procurement/33569/notice/52192/overview

Hätäkeskuslaitos (2020). Hätäpuhelun paikannus. Hätäkeskuslaitos. Viimeksi vierailtu 16.2.2022. https://112.fi/sijaintitieto

Kaupunkiliikenne (2022, tammikuu 28). HKL on nyt Kaupunkiliikenne Oy – "Nykyinen raideverkosto tulee kolminkertaistumaan seuraavan kymmenen vuoden aikana". Kaupunkiliikenne Oy. Viimeksi vierailtu 6.2.2022. https://kaupunkiliikenne.fi/yleinen/hkl-on-nyt-kaupunkiliikenne-oy-nykyinen-raideverkosto-tulee-kolminkertaistumaan-seuraavan-kymmenen-vuoden-aikana/

Katakri (2020). Tietoturvallisuuden auditointityökalu viranomaisille. Kansallinen turvallisuusviranomainen. https://um.fi/documents/35732/0/Katakri-2020_201218.pdf

Kouvola (2021, toukokuu 14). Kymmenen faktaa Kouvola RRT:stä. Kouvolan kaupunki. Viimeksi vierailtu 6.2.2022. https://www.kouvola.fi/kouvolankaupunki/strategia/karkihankkeet/rautatie-ja-maantieterminaali-kouvola-rrt/kymmenen-faktaa-kouvola-rrtsta/

Kyberturvallisuuskeskus (2021 elokuu 18). Ilmoita tietoturvapoikkeamasta (NIS-ilmoitusvelvollisuus). Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus. Viimeksi vierailtu 8.2.2022. https://www.kyberturvallisuuskeskus.fi/fi/asioi-kanssamme/ilmoita-tietoturvapoikkeamasta-nis-ilmoitusvelvollisuus?toggle=Liikenne

Liikennevirasto (2016). Saimaan kanavan liikenteenohjaus. Toteuttamisvaihtoehdot englanninkielisen linjaluotsauksen mahdollistamiseksi. Liikenneviraston tutkimuksia ja selvityksiä 56/2016.

Liikennevirasto. https://julkaisut.vayla.fi/pdf8/lts_2016-56_saimaan_kanavan_web.pdf

Liikennevirasto (2018). Liikenneviraston tutkimuksia ja selvityksiä 37/2018, Rataverkon kokonaiskuva - Lähtökohtia ja näkökulmia. https://julkaisut.vayla.fi/pdf8/lts_2018-37_rataverkon_kokonaiskuva_web.pdf

LVM (2019, maaliskuu 29). Uusi osto- ja velvoiteliikennekokonaisuus lisää merkittävästi junaliikenteen tarjontaa maakunnissa. Liikenne- ja viestintäministeriö. Viimeksi vierailtu 6.2.2022. https://www.lvm.fi/-/uusi-osto-ja-velvoiteliikennekokonaisuus-lisaa-merkittavasti-junaliikenteen-tarjontaa-maakunnissa-1003110

NCSC UK (2019, syyskuu 30). CSC CAF guidance. National Cyber Security Centre. Viimeksi vierailtu 20.2.2022. https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework

Norwegian Ministeries (2019). List of measures – National Cyber Security Strategy for Norway. Norwegian Ministeries. Viimeksi vierailtu 21.2.2022. https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/list-of-measures--national-cyber-security-strategy-for-norway.pdf

Suomen satamaliitto (2018). Suomen suurimmat satamat. Viimeksi vierailtu 8.2.2022. https://www.finnports.com/suomen-suurimmat-satamat/

Traficom (2019). Ulkomaan meriliikennetilasto 2018. Traficomin tilastoja 17/2019. Liikenne ja viestintävirasto Traficom. Viimeksi vierailtu 9.2.2022. https://www.traficom.fi/sites/default/files/media/file/Ulkomaan_Meriliikenteen_2018_vuosijulkaisu.pdf

Traficom (2020, huhtikuu 3). Elektronisten merikarttojen (ENC) jakelu. Liikenne- ja viestintävirasto Traficom. Viimeksi vierailtu 9.2.2022. https://www.traficom.fi/fi/liikenne/merenkulku/elektronisten-merikarttojen-enc-jakelu

Traficom (2020, lokakuu 15). eCall-tietopaketti pelastusviranomaisille, poliisille ja ensihoidolle. Liikenne- ja viestintävirasto Traficom. Viimeksi vierailtu 16.2.2022. https://www.traficom.fi/sites/default/files/media/publication/eCall-tietopaketti.pdf

Traficom (2021, helmikuu 6). Rataverkon haltijat perjantai 5. helmikuu 2021. Liikenne- ja viestintävirasto Traficom. Viimeksi vierailtu 6.2.2022. https://www.traficom.fi/sites/default/files/media/file/Rataverkonhaltijat Suomessa.pdf

Traficom (2021, kesäkuu 10). Uudet laivaliikenteen liikennöintivelvoitteet asetettu. Liikenne- ja viestintävirasto Traficom. Viimeksi vierailtu 9.2.2022. https://www.traficom.fi/fi/ajankohtaista/uudet-laivaliikenteen-liikennointivelvoitteet-asetettu

Traficom (2021, heinäkuu 13). Raideliikenteen turvallisuusohjelma. Liikenne- ja viestintävirasto Traficom. Viimeksi vierailtu 20.2.2022. https://www.traficom.fi/fi/liikenne/raideliikenne/raideliikenteen-turvallisuusohjelma?toggle=Luodaan%20raideliikenteen%20toimintavarmuuden%20toimintakulttuuri

Traficom (2021, elokuu 18). Ilmoita tietoturvapoikkeamasta (NIS-ilmoitusvelvollisuus). Liikenne- ja viestintävirasto Traficom. Viimeksi vierailtu 6.2.2022. https://www.traficom.fi/fi/asioi-kanssamme/ilmoita-tietoturvapoikkeamasta-nis-ilmoitusvelvollisuus?toggle=Liikenne

Sanastokeskus TSK (2017). Kokonaisturvallisuuden sanasto. TSK 50. Sanastokeskus TSK. Viimeksi vierailtu 20.2.2022. https://turvallisuuskomitea.fi/viestinta/kokonaisturvallisuuden-sanasto/

Suomen varustamot (2021). Jäsenet ja alukset. Suomen varustamot. Viimeksi vierailtu 9.2.2022. https://shipowners.fi/suomen-varustamot-ry/jasenet-ja-alukset/

Väylävirasto (2019). AIS-tiedot. Väylävirasto. Viimeksi vierailtu 10.2.2022. https://vayla.fi/vaylista/aineistot/avoindata/vesivaylatiedot/ais-tiedot

Väylävirasto (2021). Rautateiden henkilöliikenne, 1990-2020. Väylävirasto. Viimeksi vierailtu 6.2.2022. https://vayla.fi/vaylista/aineistot/tilastot/ratatilastot/rautateiden-henkilo-ja-tavaraliikenne

Väylävirasto (Päiväämätön). Digiroad - kansallinen tie- ja katuverkon tietojärjestelmä. Väylävirasto. Viimeksi vierailtu 20.2.2022. https://vayla.fi/tietoa-digiroadista

Väylävirasto (Päiväämätön). Meriliikenteen ohjaus. Väylävirasto. Viimeksi vierailtu 8.2.2022. https://vayla.fi/palveluntuottajat/ammattimerenkulku/liikkuminen-vesivaylilla/meriliikenteen-ohjaus

YourEurope (2021, lokakuu 14). Hätänumeroon 112 perustuva autojen eCall-järjestelmä. Euroopan unioni. Viimeksi vierailtu 20.2.2022. https://europa.eu/youreurope/citizens/travel/security-and-emergencies/emergency-assistance-vehicles-ecall/index_fi.htm

Oikeuskäytäntö

Tietosuojavaltuutettu. Päätös 7.12.2021. Henkilötietojen käsittelyn asianmukaisen turvallisuuden laiminlyönti ja tietoturvaloukkauksesta ilmoittamatta jättäminen. 1150/161/2021. Ei lainvoimainen.