NIS2-direktiivin vaikutukset Suomen raideliikenteen kyberturvallisuuteen

Tiina Kyrö

2025 Laurea

Laurea-ammattikorkeakoulu

NIS2-direktiivin vaikutukset Suomen raideliikenteen kybertur-vallisuuteen

Tiina Kyrö

Tietojenkäsittely

Opinnäytetyö

Maaliskuu, 2025

Laurea-ammattikorkeakoulu **Tiivistelmä**

Liiketalouden ammattikorkeakoulututkinto, tietojenkäsittely

Tradenomi (AMK)

Tiina Kyrö

NIS2-direktiivin vaikutukset Suomen raideliikenteen kyberturvallisuuteen

Vuosi 2025 Sivumäärä 27

Tämän opinnäytetyön tavoitteena oli kartoittaa, miten Euroopan Unionin päivitetyn kyberturvallisuusdirektiivin (NIS2) vaatimukset ovat vaikuttaneet Suomen raideliikenteen kyberturvallisuuteen. Opinnäytetyön tarkoituksena oli tuottaa työn tilaajalle Laurea ammattikorkeakoululle opetussisältöä logistiikka-alan koulutusohjelman suunnitteluun.

Työn tietoperusta muodostui yleisestä kyberturvallisuudesta, raideliikenteen kyberturvallisuudesta sekä NIS2-direktiivin keskeisestä sisällöstä ja sen vaatimuksista raideliikenteen kyberturvallisuuden toimijoille ja se pohjautui tutkimuskirjallisuuteen sekä luotettaviksi arvioituihin verkkolähteisiin.

Tutkimusmenetelminä työssä käytettiin laadullisen tutkimuksen menetelmiä; puolistrukturoitua haastattelua sekä teema- ja vertailuanalyysia. Työn aineistoa varten haastateltiin Suomen raideliikenteen kannalta keskeisten toimijoiden Traficomin, Väyläviraston ja Fintrafficin asiantuntijoita. Haastatteluissa kerättiin tietoa siitä, missä määrin Suomen raideliikenteen kyberturvallisuus tällä hetkellä täyttää NIS2-direktiivin vaatimukset jokaisen toimijan osalta, ja mitä haasteita toimijat olivat yhdessä ja erikseen havainneet.

Opinnäytetyön tuloksena havaittiin, että NIS2-direktiivin toteutuksen haasteissa ja vahvuuksissa oli jonkin verran vaihtelua organisaatioittain. Väylävirasto hyödyntää vahvasti jo aiemmin käyttöön otettuja viitekehyksiään, Traficom pyrkii yhä voimakkaammin sääntelyn ja raportoinnin yhtenäistämiseen, ja Fintraffic kokee turvallisuuskulttuurin muutoksen ja vanhentuneen teknologian suurimpina haasteinaan. Yhtenevää oli riskienhallinnan merkityksen korostaminen. Yhteisinä vaikeuksina koettiin turvaluokiteltujen tietojen käsittelyn rajoitukset, sekä jäsenvaltioiden vaihtelevat käytännöt, jotka molemmat vaikuttavat tiedonvaihtoon sekä organisaatioiden että jäsenmaiden välillä. Yhteisenä kyberturvallisuushuolena koettiin myös uusien osaajien koulutusvaje, joka johtaa ennen pitkää työvoimapulaan.

Opinnäytetyön kehittymisehdotuksiksi päädyttiin analyysin perusteella esittämään mm. poikkeamaraportointiprosessien yhtenäistämistä, yhtenäisten ohjeistusten laatimista sekä kansallisella tasolla että jäsenmaiden kesken, kyberturvallisuusosaamisen lisäämistä sekä yhteistyön tiivistämistä kansallisten toimijoiden välillä. Näiden kehittämisehdotusten avulla voidaan tehostaa NIS2-direktiivin toimeenpanoa Suomessa, sekä yhä vahvistaa Suomen raideliikenteen kyberturvallisuutta.

Asiasanat: raideliikenne, kyberturvallisuus, NIS2-direktiivi

Laurea University of Applied Sciences **Abstract**

Degree Programme in Business Information Technology

Bachelor's Thesis

Tiina Kyrö

The Impact of the NIS2 Directive on the Cybersecurity of Finland's Railway Sector

Year 2025 Pages 27

The objective of this thesis was to assess how the updated cybersecurity directive of the European Union (NIS2) has influenced the cybersecurity of railway sector in Finland. The aim was to provide Laurea University of Applied Sciences with educational content to support the development of degree programme in logistics.

The theoretical foundation of the study was based on general cybersecurity principles, railway cybersecurity, and the key content and requirements of the NIS2 directive for railway cybersecurity stakeholders. The knowledge base relied on academic research literature as well as reliable online sources.

This research employed qualitative methods, including semi-structured interviews, thematic analysis, and comparative analysis. Experts from the key Finnish railway cybersecurity organizations—Traficom, the Finnish Transport Infrastructure Agency (Väylävirasto), and Fintraffic—were interviewed to gather insights into the extent to which Finland's railway cybersecurity currently meets NIS2 requirements and to identify challenges encountered both individually and collectively by these organizations.

The findings revealed some variations in the challenges and strengths associated with implementing the NIS2 directive across different organizations. The Finnish Transport Infrastructure Agency relies heavily on existing cybersecurity frameworks that were already in use before the directive. Traficom is focused on further harmonizing regulatory and reporting practices.Fintraffic identified changes in cybersecurity culture and outdated technology as its primary challenges.

A shared focus across all organizations was the importance of risk management. Common difficulties included the handling of classified information and the varying cybersecurity practices of different EU member states, both of which impact information exchange between organizations and nations. Another major concern was the shortage of trained cybersecurity professionals, which is expected to lead to a workforce shortage in the future.

Based on the analysis, the following development recommendations were proposed: standardizing incident reporting processes, creating unified cybersecurity guidelines at both national and EU levels, enhancing cybersecurity expertise through education and workforce development, and strengthening collaboration among national railway cybersecurity stakeholders. These recommendations aim to facilitate the effective implementation of the NIS2 directive in Finland and further enhance the cybersecurity of Finnish railway transport.

Keywords: railway cybersecurity, NIS2 Directive

Sisällysluettelo

1 Johdanto

Digitalisaation myötä raideliikenteen infrastruktuuriin liittyvistä järjestelmistä on tullut entistä tehokkaampia ja älykkäämpiä, mikä tekee ne toisaalta myös haavoittuvammiksi erilaisille kyberhyökkäyksille, kuten haittaohjelmille, palvelunestohyökkäyksille ja tietomurroille. Raideliikenteen toimivuus on yhteiskunnan kannalta kriittinen elementti, joten kyberuhkien lisääntyessä raideliikenteen järjestelmien suojaamisesta on tullut entistä tärkeämpi osa yhteiskunnan kokonaisvaltaista resilienssiä. Tämän opinnäytetyön tavoitteena on selvittää, mitkä ovat Euroopan Unionin NIS2 (Network and Information Service Directive) -direktiivin voimaan astumisen vaikutukset Suomen raideliikenteen kyberturvallisuuteen. Opinnäytetyön tilaajana toimii Laurea ammattikorkeakoulu. Tutkimustyön tarve syntyi Laurean kiinnostuksesta ymmärtää ja analysoida NIS2-direktiivin vaikutuksia Suomen raideliikenteen kyberturvallisuuteen. Tarve liittyy erityisesti Laurean tulevaisuudessa käynnistämään logistiikka-alan koulutusohjelmaan, jossa tämän opinnäytetyön tuloksia voidaan hyödyntää opetuksen sisällön suunnittelussa. Kyberturvallisuuden kasvava merkitys logistiikka- ja liikennesektoreilla korostaa aihealueen ajankohtaisuutta ja tarpeellisuutta.

Tutkimuskysymys: Missä määrin Suomen raideliikenteen kyberturvallisuus tällä hetkellä täyttää NIS2-direktiivin vaatimukset? Tämän kysymyksen avulla pyritään saamaan kattava kuva siitä, miten hyvin direktiivin vaatimukset on toteutettu ja mitä haasteita toimeenpanossa on ilmennyt.

Opinnäytetyön aihe on rajattu koskemaan NIS2-direktiiviä ja sen vaikutuksia Suomen raideliikenteen kyberturvallisuuteen. Rajauksella keskitytään erityisesti sääntelyn asettamiin kansallisiin ja kansainvälisiin vaatimuksiin. Työ ei käsittele muiden liikennemuotojen tai EU-tason raideliikenteen kyberturvallisuutta laajemmin.

1.1 Eettiset näkökulmat

Opinnäytetyön toteutuksessa on huomioitu keskeiset eettiset näkökohdat, erityisesti tiedon käsittelyn ja raportoinnin osalta. Haastattelut toteutettiin osallistujien suostumuksella, ja tiedot anonymisoitiin luottamuksellisuuden säilyttämiseksi. Lisäksi työssä on erityisesti otettu huomioon se, ettei tutkimus muodosta riskiä Suomen raideliikenteen infrastruktuurin turvallisuudelle. Tämän vuoksi tutkimuksessa on erityisesti varottu tuottamasta tietoa, josta löytyisi yksityiskohtaisia haavoittuvuuksia tai muita tietoja, jotka mahdollistaisivat opinnäytetyön hyödyntämisen infrastruktuurin vahingoittamistarkoituksessa. Tarkat tekniset puutteet ja yksityiskohdat on jätetty kokonaan pois tutkimuksesta yhteisymmärryksessä haastateltujen kanssa. Työ keskittyy sen sijaan ylätason tarkasteluun, jossa keskitytään direktiivin

vaatimusten täyttämiseen. Tämä lähestymistapa varmistaa, että tutkimus tukee raideliikenteen kyberturvallisuuden kehittämistä ilman, että se vaarantaa raideliikenteen turvallisuutta.

2 Menetelmät

Tämän opinnäytetyön menetelminä käytetään laadullisen tutkimuksen menetelmiä; kirjallisuuskatsausta, puolistrukturoitua haastattelua, teema-analyysiä ja vertailuanalyysiä. Laadullisessa eli kvalitatiivisessa tutkimuksessa olennaista on saada esiin tutkittavien oma näkökulma tutkimuksen kohteena olevasta asiasta (Eskola & Suoranta 1998, 13). Tämän opinnäytetyön tavoitteena oli analysoida NIS2-direktiivin vaikutuksia Suomen raideliikenteen kyberturvallisuuteen, joten tutkimusmenetelmät valittiin työn tavoitetta silmällä pitäen tukemaan laadullista analyysiä, jossa painopiste on teemavertailussa ja organisaatioiden näkemyksien eroissa ja yhtäläisyyksissä. Tutkimus perustuu laadullisiin menetelmiin, koska tutkimuskohteena ovat asiantuntijoiden omakohtaiset näkemykset ja kokemukset NIS2-direktiivin toteutumisesta. Aineisto kerättiin kolmen Suomen raideliikenteen keskeisen toimijan – Traficomin, Väyläviraston ja Fintrafficin – edustajien haastattelujen avulla.

2.1 Haastattelut

Yksi yleisimpiä aineistonkeruumenetelmiä kvalitatiivisessa tutkimuksessa on haastattelu. Strukturoidussa haastattelussa kysymykset ovat kaikille haastateltaville samat ja ne esitetään samassa järjestyksessä. Esitettyihin kysymyksiin on valmiit vastausvaihtoehdot. Puolistrukturoitu haastattelu taas eroaa strukturoidusta siten, että siinä haastateltavalle ei tarjota valmiita vastausvaihtoehtoja, vaan haastateltava vastaa kysymyksiin vapaasti omilla sanoilla. (Eskola & Suoranta 1998, 63.) Tämän opinnäytetyön aineisto kerättiin puolistrukturoiduilla haastatteluilla, joissa haastateltaville esitettiin ennalta laadittuja kysymyksiä, mutta myös avoimelle keskustelulle oli tilaa. Haastateltavana oli kolme asiantuntijaa eri organisaatioista.

2.2 Teema-analyysi

Laadullisen aineiston analyysin tarkoitus on selkeyttää aineistoa ja helpottaa sitä kautta uuden tiedon luomista (Eskola & Suoranta 1998, 100). Yksi laadullisen tutkimuksen aineiston analyysitavoista on teemoittelu. (Eskola & Suoranta 1998, 116). Tässä työssä haastatteluvastaukset järjesteltiin ennalta määriteltyjen teemojen alle. Teemoittelun avulla aineistosta voitiin vertailla systemaattisesti eri organisaatioiden näkemyksiä. Vertailussa tunnistettiin selkeitä yhtenäisiä käsitteitä ja havaintoja, jotka perustuivat NIS2-direktiivin vaikutuksiin kunkin haastateltavan ja heidän edustamansa organisaation näkökulmasta.

2.3 Vertailuanalyysi

Vertailuanalyysissä tarkasteltiin haastatteluissa esiin nousseiden teemojen yhtäläisyyksiä ja eroavaisuuksia organisaatioiden välillä. Erityisesti kiinnitettiin huomiota siihen, miten eri organisaatiot ovat valmistautuneet direktiivin vaatimuksiin, sekä niiden raportointikäytäntöihin ja havaittuihin ongelmakohtiin.

3 Tietoperusta

Työn tietoperusta muodostuu muutamista tärkeimmistä käsitteistä, niiden määritelmistä ja aiheeseen liittyvästä kirjallisuudesta. Tärkeimmät työssä määriteltävät käsitteet ovat kyberturvallisuus, NIS2-direktiivi ja raideliikenteen kyberturvallisuus.

3.1 Kyberturvallisuus

Kyberturvallisuus voidaan määritellä kokoelmaksi rakenteita, prosesseja ja resursseja, joilla suojataan kybertoimintaympäristö ja siihen kuuluvat järjestelmät oikeudettomilta hyökkäyksiltä (Graigen, Diakun-Thibault & Purse 2014). Erilaiset kyberhyökkäykset voivat kohdistua ohjelmistoihin, järjestelmiin ja verkkoihin. Hyökkäysten tarkoituksena voivat olla esimerkiksi tietojen luvaton käyttö, taloudellisen hyödyn saavuttaminen, tai toiminnan häiritseminen (Cisco 2024).

Kyberturvallisuus voidaan määritellä myös laajemmin tavoitteelliseksi tilaksi, jossa kybertoimintaympäristö on luotettava ja sen toiminta on turvattu. Kyberturvallisuuteen voidaan katsoa kuuluvan ennakoivat toimenpiteet, joilla voidaan hallita ja tarpeen vaatiessa sietää erilaisia kyberhyökkäyksiä ja niiden vaikutuksia. Häiriöt kybertoimintaympäristössä aiheutuvat usein realisoituneesta tietoturvauhasta, joten kokonaisvaltaiseen kyberturvallisuuden tilaan pyrkiessä keskeinen elementti on tietoturva. Lisäksi kyberturvallisuuteen pyritään muilla toimenpiteillä kuten jatkuvuussuunnittelulla koskien kybertoimintaympäristöstä riippuvaisia fyysisiä toimintoja. Tietoturvasta puhuttaessa tarkoitetaan yleensä tiedon luottamuksellisuutta, eheyttä ja saatavuutta, kun taas kyberturvallisuudessa on kyse digitaalisen yhteiskunnan tai organisaation turvallisuutta. (Traficom 2024a.)

Euroopan Unioni on perustanut jäsenmaille yhteisen kyberturvallisuusviraston (ENISA), jonka tehtävänä on tukea EU-jäsenmaita, instituutioita ja yrityksiä kyberturvallisuuden keskeisimmillä osa-alueilla. Jäsenvaltioiden kriittisiin toimintoihin kohdistuvat kyberuhat ovat lähes poikkeuksetta rajat ylittäviä, ja aiheuttavat täten uhkaa kaikille jäsenmaille. (European Commission 2024.)

3.2 NIS2-direktiivi

NIS-direktiivien, eli Euroopan unionin kyberturvallisuusdirektiivien, taustalla on tarve kehittää koko Euroopan unionin kyberturvallisuusvalmiuksia ja siten tukea unionin kokonaisturvallisuutta sekä sen talouden ja yhteiskunnan toimintaa. Ensimmäinen, vuonna 2016 voimaan tullut NIS1-direktiivi (EU 2016/1148) edisti unionin kyberresilienssiä merkittävästi määrittämällä jäsenmaille verkko- ja tietojärjestelmien turvallisuutta koskevia strategioita ja toteuttamalla yhtenäisiä sääntelytoimenpiteitä. (EUVL L 333/80, 2.) Uudelleentarkastelu kuitenkin osoitti, että NIS1-direktiivin positiivisten vaikutusten lisäksi negatiivisia vaikutuksia havaittiin jäsenvaltioiden kansallista täytäntöönpanoa koskevissa eroissa. Kyberturvallisuusvaatimusten huomattiin vaihtelevan merkittävästi jäsenvaltioiden välillä, ja pahimmillaan jäsenvaltioiden kyberturvallisuusvaatimukset olivat jopa ristiriidassa keskenään. NIS-direktiivin täytäntöönpanon kansalliset erot aiheuttavat Euroopan unionin sisämarkkinoiden pirstoutumista, ja vaikuttavat heikentävästi erityisesti rajat ylittävään palveluntarjontaan ja kyberresilienssin tasoon koko unionin alueella. Päivitetyn, vuonna 2024 voimaan tulevan NIS2-direktiivin tavoitteena (EU 2022/2555) on täten pyrkiä poistamaan jäsenvaltioiden välisiä eroja vahvistamalla vähimmäissäännöt sääntelykehyksen toiminnalle, vahvistamalla järjestelyt kunkin jäsenvaltion vastuunviranomaisten toimivaa yhteistyötä varten, ajantasaistamalla luettelo aloista ja toiminnoista, joihin sovelletaan kyberturvallisuusvelvoitteita, ja säätämällä tehokkaista oikeussuojakeinoista ja täytäntöönpanotoimenpiteistä, jotka ovat olennaisen tärkeitä velvoitteiden tehokkaan täytäntöönpanon kannalta. (EUVL L 333/80, 3.)

3.2.1 NIS2-direktiivin soveltamisalat

NIS2- direktiiviä sovelletaan yksityisiin ja julkisiin erikseen määriteltyihin toimijoihin, jotka täyttävät suosituksen 2003/361/EY liitteessä olevan 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset tai ylittävät kyseisen artiklan 1 kohdassa säädetyt keskisuurten yritysten määrittelyssä käytettävät kynnysarvot. Keskisuuriksi yrityksiksi määritellään suosituksen mukaan yritykset, joilla on vähemmän kuin 250 työntekijää ja joiden vuosiliikevaihto on enintään 50 miljoonaa euroa, tai taseen loppusumma on enintään 43 miljoonaa euroa. Suuremmiksi toimijoiksi määritellään yritykset, jotka ylittävät nämä kriteerit. (2003/361/EY, s. 36–41.)

NIS2- direktiivin soveltamisalaan kuuluvat yksityiset ja julkiset erikseen määritellyt toimijat on jaettu kahteen kategoriaan: tärkeisiin ja keskeisiin toimijoihin. Keskeisiksi toimijoiksi direktiivin kolmannessa artiklassa on määritelty keskisuuren yrityksen määritelmän täyttävät ja ylittävät erittäin kriittiset toimialat, eli energia, liikenne, pankkitoiminta, finanssimarkkinoiden infrastruktuurit, terveys, juomavesi, jätevesi, digitaalinen infrastruktuuri, tieto- ja viestintätekniikkapalvelujen hallinta, julkishallinto, ja avaruus. (EUVL L 333/80, liite 1.) Sen lisäksi keskeisiksi toimijoiksi luetaan hyväksytyt luottamuspalvelun tarjoajat,

aluetunnusrekisterit ja domain name system-palveluntarjoajat niiden koosta riippumatta, yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat jotka täyttävät keskisuuren yrityksen tai sen ylittävän määritelmän, julkishallinnon toimijat jonka jäsenvaltio on kansallisen lainsäädäntönsä perusteella määritellyt keskustason julkishallinnon toimijaksi tai aluetason toimijaksi jonka toiminnan häiriintymisellä voisi olla merkittävä vaikutus yhteiskunnan tai talouden kriittisiin toimintoihin. Lisäksi jäsenvaltioille on jätetty oikeus kansallisen lainsäädäntönsä nojalla arvioida keskeisiksi toimijoiksi toimijat, jotka tarjoavat ainoana jäsenvaltiossa kriittistä palvelua, joka on olennainen yhteiskunnan tai talouden toimivuuden kannalta, jos kyseisen toimijan palvelussa esiintyisi häiriö, sillä voisi olla merkittäviä vaikutuksia yleiseen järjestykseen, turvallisuuteen tai kansanterveyteen tai häiriö voisi aiheuttaa merkittävän systeemisen riskin, erityisesti aloilla, joilla vaikutukset voisivat ulottua myös rajojen yli, tai toimija on myös kriittinen kansallisella tai alueellisella tasolla sen erityisen suuren merkityksen vuoksi kyseiselle toimialalle tai muille riippuvaisille aloille. (EUVL L 333/80, 31.)

Tärkeiksi toimijoiksi NIS2-direktiivin kolmannessa artiklassa on määritelty muut kriittiset toimialat, eli posti- ja kuriiripalvelut, jätehuolto, kemikaalien valmistus, tuotanto ja jakelu, elintarvikkeiden tuotanto, jalostus ja jakelu, valmistuspalvelut, digitaalisen palvelun tarjoajat, ja tutkimustoiminta (EUVL L 333/80, liite 2). Sen lisäksi tärkeiksi toimijoiksi luetaan myös erittäin kriittisiksi listatut toimialat, jotka eivät täytä keskisuuren yrityksen tai sen ylittävää määritelmää. Lisäksi jäsenvaltioille on jätetty oikeus kansallisen lainsäädäntönsä nojalla arvioida tärkeiksi toimijoiksi toimijat, jotka tarjoavat ainoana jäsenvaltiossa kriittistä palvelua, joka on olennainen yhteiskunnan tai talouden toimivuuden kannalta, jos kyseisen toimijan palvelussa esiintyisi häiriö, sillä voisi olla merkittäviä vaikutuksia yleiseen järjestykseen, turvallisuuteen tai kansanterveyteen tai häiriö voisi aiheuttaa merkittävän systeemisen riskin, erityisesti aloilla, joilla vaikutukset voisivat ulottua myös rajojen yli, tai toimija on myös kriittinen kansallisella tai alueellisella tasolla sen erityisen suuren merkityksen vuoksi kyseiselle toimialalle tai muille riippuvaisille aloille. (EUVL L 333/80, 31.)

NIS2- direktiivin toisessa artiklassa mainitaan, että direktiivi ei velvoita julkishallinnon toimijoita, jotka toimivat kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla, mukaan lukien rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet (EUVL L 333/80, 30).

Yllä olevien keskeisten ja tärkeiden toimijoiden määritelmien lisäksi direktiivin toiseen artiklaan on sisällytetty kuitenkin useita poikkeuksia. NIS2-direktiiviä sovelletaan toiminnan koosta riippumatta myös seuraavissa tapauksissa, jotka on havainnollistettu taulukossa 1.

Poikkeus	Kuvaus
Ainoa palveluntarjoaja	”Toimija on ainoa, joka tarjoaa kyseistä palvelua jäsenvaltiossa, ja palvelu on välttämätön yhteiskunnan tai talouden kriittisten toimintojen ylläpitämiseksi.”
Merkittävä vaikutus yhteiskuntaan	”Toimijan palvelussa esiintyvä häiriö voisi merkittävästi vaikuttaa yleiseen järjestykseen, turvallisuuteen tai kansanterveyteen.”
Systeeminen riski	”Toimijan palvelussa esiintyvä häiriö voisi aiheuttaa merkittävän systeemisen riskin, erityisesti aloilla, joilla häiriöllä voisi olla rajat ylittäviä vaikutuksia.”
Toimijan suuri kansallinen tai alueellinen merkitys	”Toimijalla on erityisen suuri merkitys kansallisella tai alueellisella tasolla kyseisen toimialan, palvelutyypin tai muiden keskinäisriippuvaisten toimialojen kannalta.”
Viestintäverkot ja niihin liittyvät palvelut	”Palvelujen tarjoajat ovat yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajia, luottamuspalvelun tarjoajia tai aluetunnusrekisterejä ja DNS (eli domain name system) palveluntarjoajia, tai toimija tarjoaa verkkotunnusten rekisteröintipalveluja.”

Julkishallinnon toimija ja riskiperuste	”Toimija on julkishallinnon toimija, jonka jäsenvaltio on kansallisen lainsäädäntönsä mukaisesti määritellyt keskustason julkishallinnon toimijaksi tai jonka jäsenvaltio on kansallisen lainsäädäntönsä mukaisesti määritellyt aluetason julkishallinnon toimijaksi ja joka riskiperusteisen arvioinnin perusteella tarjoaa palveluja, joiden häiriintymisellä voisi olla merkittävä vaikutus yhteiskunnan tai talouden kriittisiin toimintoihin.”

Taulukko 1: NIS2 soveltaminen toimijan koosta riippumatta (EUVL L 333/80, 30)

Jäsenvaltioille itselleen on jätetty harkintavalta päättää ulottavatko he kansallisessa lainsäädännössään NIS2-direktiivin koskemaan myös paikallistason julkishallinnon toimijoita, ja opetus- ja koulutusalan laitoksia (EUVL L 333/80, 30).

3.2.2 NIS2-direktiivin vaatimukset jäsenvaltioille

NIS2-direktiivi asettaa alkuperäisen tavoitteensa mukaan jäsenvaltioille useita vaatimuksia kyberturvallisuuden tason yhdenmukaistamiseksi ja ristiriitojen poistamiseksi. Direktiivi lähtee liikkeelle jäsenvaltioiden kansallisten kyberturvallisuusstrategioiden yhdenmukaistamisesta. Jokaisen jäsenvaltion on hyväksyttävä kansallinen kyberturvallisuusstrategia, jossa määritetään strategiset tavoitteet, kyseisten tavoitteiden saavuttamiseksi tarvittavat resurssit sekä asianmukaiset politiikka- ja sääntelytoimenpiteet kyberturvallisuuden korkean tason saavuttamiseksi ja ylläpitämiseksi. Direktiivi velvoittaa jäsenvaltioita myös auditoimaan kansallisia kyberturvallisuusstrategioitaan säännöllisesti, ja tarvittaessa ajantasaistamaan strategioitaan viiden vuoden välein. (EUVL L 333/80, 36.)

Jokaisen jäsenvaltion on nimettävä tai perustettava yksi tai useampi toimivaltainen viranomainen, joka vastaa kyberturvallisuudesta ja valvoo tämän direktiivin täytäntöönpanoa kansallisella tasolla. Kunkin jäsenvaltion on nimettävä tai perustettava myös keskitetty yhteyspiste. Jos jäsenvaltio nimeää tai perustaa vain yhden kyberturvallisuutta ja tämän direktiivin täytäntöönpanoa valvovan toimivaltaisen viranomaisen, kyseinen toimivaltainen viranomainen toimii myös kyseisen jäsenvaltion keskitettynä yhteyspisteenä. Jäsenvaltioiden on varmistettava, että niiden toimivaltaisilla viranomaisilla ja keskitetyllä yhteyspisteellä on riittävät resurssit toimittaa niille osoitetut tehtävät tuloksekkaasti ja tehokkaasti ja siten saavuttaa NIS2- direktiivin tavoitteet. (EUVL L 333/80, 37.)

Jokaiseen jäsenvaltioon on nimettävä tai perustettava yksi tai useampi kyberkriisinhallintaviranomainen. Kyberkriisinhallintaviranomainen on toimivaltainen viranomainen, joka vastaa laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallinnasta. Kunkin jäsenvaltion on myös yksilöitävä valmiudet, voimavarat ja menettelyt, joita voidaan käyttää kriisitilanteissa tämän direktiivin soveltamiseksi. Kunkin jäsenvaltion on laadittava kansallinen laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallintasuunnitelma, jossa vahvistetaan laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallinnan tavoitteet ja järjestelyt. (EUVL L 333/80, 38.)

Jokaisen jäsenvaltion on perustettava tai nimettävä yksi tai useampi tietoturvaloukkauksiin reagoiva ja niitä tutkiva yksikkö, eli CSIRT (Computer Security Incident Response Team) yksikkö (EUVL L 333/80, 38). CSIRT-yksiköiden keskeisimpiä tehtäviä ovat kyberuhkien, haavoittuvuuksien ja poikkeamien seuranta ja analysointi kansallisella tasolla, kyberturvallisuuspoikkeamiin reagointi, kyberturvallisuuden tilannekuvan ylläpito, kyberuhkia, haavoittuvuuksia ja poikkeamia koskevien ennakkovaroitusten ja hälytysten antaminen keskeisille ja tärkeille toimijoille sekä toimivaltaisille viranomaisille ja muille asianomaisille sidosryhmille. (EUVL L 333/80, 39). Huomioitavaa on, että direktiivi ohjaa jäsenvaltioita kiinnittämään huomiota kansallisen tason yhteistyöhön kyberturvallisuusviranomaisten kesken, sillä mikäli saman jäsenvaltion toimivaltaiset viranomaiset, keskitetty yhteyspiste ja CSIRT-yksiköt ovat toisistaan erillisiä, niiden on tehtävä yhteistyötä keskenään tässä direktiivissä säädettyjen velvoitteiden täyttämiseksi (EUVL L 333/80, 41).

3.2.3 NIS2-direktiivin vaatimukset toimijoille

NIS2-direktiivi velvoittaa EU:n jäsenvaltioita varmistamaan, että direktiivissä luetellut keskeiset ja tärkeät toimijat toteuttavat asianmukaiset ja oikeasuhteiset tekniset, operatiiviset ja organisatoriset toimenpiteet hallitakseen riskejä, joita heidän toiminnoissaan tai palveluntarjonnassaan käyttämien verkko- ja tietojärjestelmien turvallisuuteen kohdistuu, ja estääkseen tai minimoidakseen poikkeamien vaikutukset palvelujensa vastaanottajiin ja muihin palveluihin. Toimenpiteiden oikeasuhteisuutta arvioitaessa on huomioitava, missä määrin toimija altistuu riskeille, toimijan koko ja poikkeamien esiintymisen todennäköisyys ja niiden vakavuus, mukaan lukien niiden yhteiskunnalliset ja taloudelliset vaikutukset. (EUVL L 333/80, 48.)

Direktiivissä on myös säädetty eri valvontajärjestelmistä keskeisille ja tärkeille toimijoille. Keskeisiin toimijoihin sovelletaan kattavaa valvontajärjestelmää, johon kuuluu etukäteis- ja jälkikäteisvalvonta. Tärkeisiin toimijoihin sovelletaan kevyempää valvontajärjestelmään, joka sisältää vain jälkikäteisvalvonnan. Kahdentasoisen valvontajärjestelmän tarkoituksena on varmistaa kyseisten toimijoiden ja toimivaltaisten viranomaisten velvoitteiden oikeudenmukainen tasapaino. (EUVL L 333/80, 25.)

Velvoittavien oikeasuhtaisten toimenpiteiden on perustuttava kaikki vaaratekijät huomioivaan toimintamalliin. Toimintamallin tavoitteena on suojata verkko- ja tietojärjestelmät, sekä näiden järjestelmien fyysinen ympäristö poikkeamilta. NIS2- direktiivin asettamat vähimmäisvaatimukset kyseisille toimenpiteille on esitetty taulukossa 2.

Artikla 21, kohta 2, alakohta	Vaatimus	Kuvaus
a)	Riskienhallinta ja tietoturvapolitiikat	”Riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat politiikat”
b)	Poikkeamien huomioiminen	”Poikkeamien käsittely”
c)	Jatkuvuudenhallinta ja kriisinhallinta	”Toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta”
d)	Toimitusketjun turvallisuus	”Toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat”
e)	Verkko- ja tietojärjestelmien kokonaisvaltainen turvallisuus	”Verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen”
f)	Kyberturvallisuustoimenpiteiden arviointi	”Toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta”

g)	Kyberhygienia ja koulutus	”Perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus”
h)	Kryptografian ja salauksen käyttö	”Toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä”
i)	Henkilöstöturvallisuus ja pääsynhallinta	”Henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta”
j)	Monivaiheinen tunnistautuminen ja turvallinen viestintä	”Tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa”

Taulukko 2: NIS2-direktiivin asettamat vähimmäisvaatimukset (EUVL L 333/80, 48)

NIS2-direktiivi asettaa myös keskeisille ja tärkeille toimijoille raportointivelvoitteen merkittävistä poikkeamista. Poikkeamasta on ilmoitettava ilman aiheetonta viivytystä CSIRT-yksikölle tai tapauksen mukaan toimivaltaiselle viranomaiselle. Poikkeama katsotaan merkittäväksi, mikäli se on aiheuttanut tai voi aiheuttaa vakavan toimintahäiriön tai asianomaiselle toimijalle taloudellisia tappioita. Samoin poikkeama katsotaan merkittäväksi, jos se on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa. Toimijan on ilman aiheetonta viivytystä ja joka tapauksessa 24 tunnin kuluessa siitä, kun poikkeama on tullut tietoon, raportoitava ennakkovaroitus, jossa on ilmoitettava, epäilläänkö poikkeaman johtuvan lainvastaisista tai vihamielisistä teoista, tai voiko sillä olla rajat ylittäviä vaikutuksia. Seuraava poikkeamailmoitus on annettava ilman aiheetonta viivytystä ja joka tapauksessa 72 tunnin kuluessa poikkeaman havaitsemisesta, ja siinä on otettava kantaa poikkeaman vakavuuteen ja vaikutuksiin, sekä vaarantumisindikaattoriin. Viimeiseksi on vielä toimitettava loppuraportti viimeistään kuukauden kuluessa poikkeamailmoituksen toimittamisesta. (EUVL L 333/80, 50.)

3.3 Raideliikenteen kyberturvallisuus

Raideliikenteen kyberturvallisuus voidaan määritellä junaliikenteen digitaalisten järjestelmien, ratasensorien, ohjausmekanismien ja fyysisen infrastruktuurin suojaamiseksi kyberuhkia vastaan. Raideliikenteen kyberturvallisuuden voidaan katsoa kattavan niin fyysisen turvallisuuden, kuin myös verkko- ja tietoturvajärjestelmät sekä erilaiset tiedonsuojausprotokollat ja sen kokonaisvaltaisena tavoitteena on suojata raideliikenteen infrastruktuuria kyberhyökkäyksiltä ja minimoida siihen kohdistuvia riskejä. (Ibadah, Benavente-Peces & Pahl 2024.)

Keskeisiksi osa-alueiksi raideliikenteen kyberturvallisuudessa on tunnistettu ennalta ehkäisevät toimenpiteet, riskienhallinta, kyberturvallisuuskulttuuri ja turvallisuuden huomiointi suunnittelussa (Safety by Design). Raideliikenteen kyberturvallisuuden erityispiirteitä yleiseen kyberturvallisuuteen nähden muodostavat mm. raideliikenteen infran pitkä käyttöikä, laitteiden monimutkaisuus ja keskinäinen riippuvuus sekä vanhojen ja uusien järjestelmien yhdistäminen. Raideliikenteen infrastruktuurin laitteiden suunniteltu käyttöikä on vuosikymmeniä, kun taas kyberuhat kehittyvät jatkuvasti. Raideliikenteeseen liittyvät liikenteenohjausjärjestelmät, erilaiset sensorit ja junakalusto muodostavat monimutkaisen kokonaisuuden, jonka suojaaminen vaatii kattavaa kyberturvallisuusstrategiaa. Haasteena raideliikenteen kyberturvallisuudessa on myös vanhat järjestelmät ja niiden liittäminen osaksi uusia teknologioita. Näissä prosesseissa saattaa muodostua tietoturva-aukkoja, joita erilaiset standardit eivät kata. (Ibadah, Benavente-Peces & Pahl 2024.)

Raideliikenteen kyberturvallisuuteen kohdistuu riskejä, jotka voivat potentiaalisesti aiheuttaa vahinkoa fyysiseen maailmaan, raideliikenteen turvallisuuteen ja toimintavarmuuteen. Raideliikennejärjestelmän eri toimijoiden keskeisenä tehtävänä on tunnistaa ja hallita näitä riskejä, koska kyberturvallisuus tunnetaan nykyään osana raideliikenteen kokonaisturvallisuutta. Suomessa Traficom vastaa raideliikenteen kyberturvallisuuden kehittämisestä ja koordinoinnista, sekä ennaltaehkäistä tietoturvaloukkauksia, tiedottaa tietoturva-asioista ja selvittää tietoturvaloukkauksia ja niiden uhkia. Traficom toimii kansallisena kyberturvallisuuskeskuksena. (Traficom, 2024a.)

3.3.1 Esimerkkejä raideliikenteeseen kohdistuneista kyberhyökkäyksistä maailmalla

Lokakuussa 2017 Ruotsissa tapahtui kaksi palvelunestohyökkäystä raideliikenteeseen kohdistuen. Ensimmäinen hyökkäys tapahtui 11. lokakuuta ja vaikutti Ruotsin liikennevirastoon (Trafikverket) sen kahden internet-palveluntarjoajan kautta. Hyökkäys kaatoi junien sijaintipalvelun, viraston sähköpostijärjestelmän, verkkosivuston ja liikennöintikartat. Asiakkaat eivät tänä aikana voineet esimerkiksi tehdä varauksia tai saada päivityksiä viivästyksistä. Tämän seurauksena junaliikenne ja muut palvelut jouduttiin hoitamaan manuaalisten varausjärjestelmien kautta. Seuraavana päivänä tapahtui toinen laajennettu palvelunestohyökkäys, joka vaikutti Ruotsin liikenneviraston verkkosivustoon. Ruotsin liikennevirasto on erillinen

viranomainen, joka vastaa liikennejärjestelmien sääntelystä ja tarkastuksesta. Hyökkäys vaikutti myös Länsi-Ruotsin julkisen liikenteen operaattori Vasttrafikiin, mikä johti lipunmyyntisovelluksen ja verkkopohjaisen matkasuunnittelupalvelun kaatumiseen. (Enisa 2020, 14.)

Toukokuussa 2018 Tanskassa tapahtui laajennettu palvelunestohyökkäys, joka vaikutti raideliikenteen lipunmyyntijärjestelmiin. Tanskalaiset matkustajat eivät voineet ostaa lippuja lippuautomaateista, verkkosovelluksesta, verkkosivustolta tai tietyistä asemakojuista. On arvioitu, että noin 15 000 asiakasta kärsi tästä. (Enisa 2020, 14.)

Maaliskuussa 2020 Yhdistynyt kuningaskunta koki rautatieasemien ilmaisiin Wi-Fi-palveluiden asiakastietoihin kohdistuvan tietovuodon. Noin 10 000 henkilön sähköpostiosoitteet ja matkustustiedot, jotka käyttivät Yhdistyneen kuningaskunnan rautatieasemien tarjoamaa ilmaista Wi-Fi-palvelua, vuotivat verkkoon. Network Rail ja palveluntarjoaja C3UK vahvistivat tapauksen. Tietokannassa oli 146 miljoonaa tietuetta, mukaan lukien henkilökohtaiset yhteystiedot ja syntymäajat. Tietomurto koski myös sovellusta "Indian Rail", joka on suosittu sovellus Applen App Storessa. Tietomurto johtui paljastuneesta Firebase-tietokannasta, joka sisälsi 2 357 684 riviä sähköposteja, käyttäjänimiä ja selkokielisiä salasanoja. (Enisa 2020, 14.)

3.4 Tietoperustan synteesi

Tämän opinnäytetyön tietoperustan muodostavat NIS2-direktiivin tavoitteet, kyberturvallisuuden määritelmä ja raideliikenteen kyberturvallisuuden määritelmä. Tietoperustassa korostuivat kolme näkökulmaa: tekniset näkökulmat, organisatoriset näkökulmat ja datan hallinnan näkökulmat.

3.4.1 Tekninen näkökulma

NIS2-direktiivin tekniset vaatimukset painottuvat verkko- ja tietojärjestelmien turvallisuuden yhtenäistämiseen. Suomen raideliikenteen osalta tämä tarkoittaa ennen kaikkea vanhentuneiden rautatieteknologioiden päivittämistä, sillä niiden haavoittuvuus lisää väistämättä riskejä ja vaikeuttaa direktiivin asettamien standardien noudattamista. Teknologian modernisoinnin rinnalla kansainvälisesti tunnustettujen standardien, kuten ISO27001, laajempaa soveltamista pidetään suositeltavana. Lisäksi teoria korostaa teknologian jatkuvaa kehittämistä uusien kyberuhkien torjumiseksi.

3.4.2 Organisatoriset näkökulmat

NIS2-direktiivi tuo mukanaan organisatorisia vaatimuksia, kuten selkeämmän vastuunjaon ja toimivamman yhteistyön eri toimijoiden välillä. Raideliikenteen kentässä tämä on erityisen tärkeää, sillä toimijat, kuten Traficom, Väylävirasto ja Fintraffic, ovat riippuvaisia toisistaan. Direktiivi korostaa, että onnistunut kyberturvallisuustyö edellyttää toimivaa koordinaatiota organisaatioiden välillä sekä toimivien yhteistyörakenteiden kehittämistä kansallisesti ja

kansainvälisesti. Näiden lisäksi organisaatioiden kyky vastata raportointivaatimuksiin ja poikkeamien hallintaan ovat avainasemassa direktiivin toimeenpanossa.

3.4.3 Datanhallinnan näkökulma

Tietoperustassa havaittiin, että erityisesti turvaluokitellun tiedon käsittelyssä on vielä kehittämistarpeita. Tämä korostuu sekä kansallisessa että EU-tason yhteistyössä, koska käytännöt vaihtelevat ja tiedon jakamiseen liittyy lainsäädännöllisiä esteitä. Samalla tiedonvaihdon tehokkuus ja tilannekuvan ylläpito nähtiin kriittisinä tekijöinä kyberturvallisuuden vahvistamisessa.

4 Puolistrukturoitu haastattelu

Haastattelut olivat opinnäytetyön keskeinen tutkimusmenetelmä, ja niiden avulla kartoitettiin NIS2-direktiivin vaikutuksia Suomen raideliikenteen kyberturvallisuuteen keskeisten organisaatioiden näkökulmasta. Puolistrukturoidut haastattelut mahdollistivat sekä valmiiden kysymysten esittämisen että joustavan keskustelun, jossa haastateltavat saattoivat nostaa esiin itselleen tärkeitä teemoja. Näin saatiin monipuolinen ja syvällinen kuva direktiivin vaikutuksista ja siihen liittyvistä käytännön haasteista.

4.1 Haastateltavien valinta ja tarkoituksenmukaisuus

Haastateltavat valittiin harkinnanvaraisella otannalla opinnäytetyön tavoite huomioiden. Haastateltavat valittiin sillä perusteella, että heiltä oletettiin saatavan ajantasaista ja tarkkaa tietoa edustamiensa organisaatioiden käytännöistä ja toiminnasta suhteessa työn tutkimuskysymykseen. Ennen haastateltavien valintaa tunnistettiin Suomen raideliikenteen kyberturvallisuuden kannalta keskeisiksi toimijoiksi Traficom, Väylävirasto ja Fintraffic. Jokaisesta organisaatiosta haastateltiin yksi asiantuntija.

Traficom on virallinen kyberturvallisuutta valvova viranomainen Suomessa, joka vastaa mandaattinsa mukaisesti NIS2-direktiivin sääntelyn ja raportoinnin kehittämisestä. Väylävirasto on Suomen rataverkon infrastruktuurista vastaava organisaatio, jolla on merkittävä rooli raideliikenteen kyberturvallisuuden hallinnassa. Fintraffic taas on liikenteenohjauspalveluiden tuottaja, joka vastaa operatiivisesta turvallisuudesta yhteistyössä Väyläviraston kanssa. (Traficom 2024a; Traficom 2024b.)

Näiden kohdeorganisaatioiden valinta perustui niiden keskeisiin rooleihin NIS2-direktiivin täytäntöönpanossa. Organisaatioiden edustajien näkökulmat tarjosivat kattavan kuvan direktiivin vaikutuksista raideliikenteen kyberturvallisuuden eri toimintatasoilla, kuten esimerkiksi sääntely, infrastruktuuri ja operatiivinen toiminta. Haastateltavat valittiin kontaktoimalla edellä

mainittuja organisaatioita ja etsimällä kustakin organisaatiosta henkilö, joka parhaiten osasi vastata aiheeseen liittyviin haastattelukysymyksiin.

4.2 Haastatteluprosessi

Haastattelut toteutettiin lokakuussa 2024, ja ne suoritettiin etäyhteyksin, mikä mahdollisti osallistujien joustavan aikatauluttamisen. Kullekin haastattelulle varattiin aikaa noin tunti, ja haastattelut dokumentoitiin huolellisesti tekemällä muistiinpanoja. Muistiinpanot käytiin haastattelujen jälkeen vielä yhdessä haastateltavan kanssa läpi tiedon oikeellisuuden varmistamiseksi. Haastattelukysymykset laadittiin ennalta teemojen mukaisesti, ja ne kattoivat kuviossa 1 esitetyt teemat.

Kuvio 1: Haastattelujen teemat

Haastattelujen teemoiksi valikoituivat NIS2-direktiivin vaatimusten toteutus, valvontajärjestelmät ja raportointivelvollisuudet, haasteet ja kehitystarpeet, yhteistyö ja sidosryhmät sekä kyberturvallisuuden hallinta, sillä niiden avulla oletettiin saatavan relevanttia tietoa tutkimusongelmaan liittyen. Asiantuntijoiden haastattelun avulla saatiin selkeä kuva siitä, miten kussakin kohdeorganisaatiossa on huomioitu NIS2-direktiivi ja sen vaatimukset. Aineistolle

suoritetussa teema- ja vertailuanalyysissa kyettiin tunnistamaan yhteneväisyyksiä ja eroavaisuuksia organisaatioiden välillä.

4.3 Teema-analyysi

Haastatteluvastaukset järjesteltiin ennalta määriteltyjen teemojen alle. Näiden teemojen tarkoitus oli strukturoida aineisto niin, että eri organisaatioiden näkemyksiä voitiin vertailla systemaattisesti keskenään. Analyysissä tunnistettiin toistuvia käsitteitä ja poikkeavuuksia, jotka kuvastavat NIS2-direktiivin vaikutuksia. Teema-analyysin avulla haastatteluaineisto kategorisoitiin viiteen keskeiseen teemaan: NIS2-vaatimusten toteutus, valvontajärjestelmät ja raportointivelvollisuudet, haasteet ja kehitystarpeet, yhteistyö ja sidosryhmät sekä kyberturvallisuusuhkien hallinta.

Aineiston perusteella kaikki toimijat korostivat riskienhallinnan merkitystä, mutta lähestymistavat erosivat organisaatiokohtaisesti. Väylävirasto hyödyntää jo aiemmin käyttöön ottamaansa ISO27001-viitekehystä, kun taas Fintraffic on vasta aloittamassa tämän järjestelmän integrointia. Haasteista Fintraffic nosti esille turvallisuuskulttuurin muutoksen, koska kyberturvallisuudelle ei ole aiemmin annettu riittävää painoarvoa. Traficom taas painottaa, että toimijoiden oma riskienhallinta on ensisijaista. NIS2 ei ole aiheuttanut suuria muutoksia Väylävirastolle, mutta Fintraffic ja Traficom joutuvat mukauttamaan toimintatapojaan merkittävästi. Traficom on ottanut käyttöön NIS-raportointijärjestelmän, mutta muiden toimijoiden käytännöt vaihtelevat. Väylävirasto korostaa kevyttä raportointimallia, ja Fintraffic taas käyttää jo olemassa olevia häiriöilmoitusjärjestelmiä. Suomen linja raportoida myös teknisiä häiriöitä on ollut kiistanalainen. Osa jäsenmaista raportoi vain kyberturvallisuushyökkäyksistä, mutta Traficomin linjauksella Suomi raportoi myös teknisistä häiriöistä. Väylävirasto ja Fintraffic ovat joutuneet mukauttamaan käytäntöjään Traficomin vaatimusten mukaisesti.

Kaikki toimijat kohtaavat haasteita vanhan teknologian päivittämisessä NIS2-vaatimusten tasolle. Väylävirasto korvaa teknologian puutteet riskienhallinnalla. Kyberturvallisuus- ja raideliikenneosaajien puute hidastaa kehitystä, erityisesti Fintrafficin ja Väyläviraston näkökulmasta. NIS2-direktiivi on parantanut kansallista yhteistyötä entuudestaan. Toimijat, kuten Väylävirasto ja Fintraffic, ovat muodostaneet uusia yhteistyöryhmiä. Tiedonvaihto on kuitenkin joiltakin osin yhä haastavaa turvaluokiteltujen tietojen osalta. Fintraffic on kehittänyt uhkatilannekuvan hallintaa, mutta toiminta on vielä alkuvaiheessa. Väylävirasto ja Traficom panostavat enemmän ennakoivaan toimintaan. Kaikki toimijat pitävät nopeita raportointivaatimuksia (esim. 72 tuntia) haastavina erityisesti viikonloppuisin ja lomakausina.

4.2 Vertailuanalyysi

Vertailuanalyysissä tarkasteltiin NIS2-direktiivin vaikutuksia eri organisaatioihin vertaamalla niiden näkemyksiä ja käytäntöjä keskeisissä teemoissa, kuten riskienhallinnassa,

raportointikäytännöissä ja yhteistyössä. Aineisto analysoitiin koodaamalla haastatteluvastaukset teemoihin ja tunnistamalla niistä sekä yhtäläisyyksiä että eroavaisuuksia. Vertailussa huomioitiin myös kunkin organisaation toimintaympäristö ja vastuualueet.

Vertailuanalyysissä tarkasteltiin haastatteluissa esiin nousseiden teemojen yhtäläisyyksiä ja eroavaisuuksia organisaatioiden välillä. Erityisesti kiinnitettiin huomiota siihen, miten eri organisaatiot ovat valmistautuneet direktiivin vaatimuksiin, sekä niiden raportointikäytäntöihin ja haasteisiin. Vertailuanalyysissa havaittiin yhtäläisyyksiä ja eroja on esitetty taulukossa 3.

Osa-alue	Yhtäläisyydet	Erot
Riskienhallinta	Kaikki toimijat painottavat riskienhallinnan merkitystä, mutta toteutustavat eroavat.	-
Suojausmenetelmät	Kaikille on yhteistä, että teknisten puutteiden kompensoimiseksi käytetään muita suojausmenetelmiä.	-
Kyberturvallisuusosaajien puute	Kaikki haastateltavat tunnistavat kyberturvallisuusosaajien puutteen suureksi ongelmaksi. Lisää ammattilaisia alalle kaivataan osaamisen ja tulevaisuuden työvoiman turvaamiseksi.	-
Tiedonvaihto	Vaikka tiedonvaihtokäytännöt ovat jokseenkin toimivia kansallisella tasolla, EU-tasolla turvaluokittelut aiheuttavat yhä ongelmia jäsenmaiden välillä. Tietoa ei voida täysimääräisesti edelleenkään vaihtaa.	-

Raportointikäytännöt	-	Väylävirasto ja Fintraffic käyttävät raportoinnissaan kevyempiä malleja, kun taas Traficom korostaa kattavaa raportointia teknisistä häiriöistä. Tämä on johtanut erilaisiin toimintamalleihin.
NIS2-vaikutukset	-	Väylävirasto kokee, että NIS2 ei juuri muuta heidän toimintaansa, sillä tarvittavat viitekehykset NIS2 vaatimusten täyttämiseksi olivat jo entuudestaan käytössä. Fintraffic ja Traficom sen sijaan joutuvat tekemään merkittäviä mukautuksia toimintaansa.
Uhkatilannekuvan ylläpito	-	Fintraffic on toimijoista ainoa, joka mainitsee kattavan uhkatilannekuvan ylläpidon ja hallinnan yhtenä tavoitteenaan.

Taulukko 3: Kohdeorganisaatioiden yhtäläisyydet ja erot haastatteluaineiston perusteella

Vertailu osoittaa, että NIS2-direktiivin vaikutukset vaihtelevat toimijasta riippuen. Traficomilla on vahva rooli valvovana viranomaisena, joten se painottaa laajaa raportointia ja tiukkaa sääntelyä. Väylävirasto ja Fintraffic keskittyvät enemmän sisäisten prosessiensa ja resurssiensa kehittämiseen vaadittavalle tasolle.

5 Tulokset

Haastattelujen perusteella selvisi, että NIS2-direktiivin vaikutukset Suomen raideliikenteen kyberturvallisuuteen vaihtelevat organisaatiosta riippuen. Kaikki haastatellut korostivat riskienhallinnan keskeistä roolia direktiivin vaatimusten täyttämisessä, mutta toimintamallit ja painotukset eroavat. Traficom nosti esiin ennakkovalvonnan puutteen ja painotti toimijoiden omaa vastuuta riskienhallinnasta. Väylävirasto puolestaan on integroinut NIS2-vaatimukset

olemassa oleviin prosesseihinsa, minkä ansiosta työllistävät vaikutukset ovat olleet vähäisiä. Fintraffic puolestaan koki kulttuurinmuutoksen ja vanhan teknologian päivittämisen suurimmiksi haasteikseen. Raportointikäytännöissä oli havaittavissa yhteneväisyyksiä: kaikki toimijat hyödyntävät olemassa olevia järjestelmiä, mutta Traficom painottaa teknisten häiriöiden raportointia, mikä on herättänyt keskustelua EU:n sisällä. Lisäksi haastateltavat toivat esiin osaajapulan ja turvaluokitellun tiedon käsittelyn ongelmat merkittävinä hidasteina direktiivin täytäntöönpanossa. Positiivisena kehityksenä nähtiin sidosryhmien yhteistyön vahvistuminen, mikä on johtanut tiedonvaihdon parantumiseen ja yhteisiin kyberturvallisuusharjoituksiin.

Vertailuanalyysi osoitti selkeitä yhtäläisyyksiä ja eroavaisuuksia organisaatioiden välillä. Kaikki toimijat korostivat riskienhallinnan merkitystä ja tunnistivat osaajapulan haasteeksi, mutta niiden valmiudet täyttää NIS2-direktiivin vaatimuksia vaihtelivat. Väylävirasto oli vähiten riippuvainen direktiivin ohjeistuksesta, sillä sen nykyiset viitekehykset, kuten ISO27001, ovat jo linjassa vaatimusten kanssa. Traficom puolestaan keskittyi erityisesti sääntelyn kehittämiseen ja kattavaan raportointiin, kun taas Fintraffic korosti yhteistyötä muiden sidosryhmien kanssa ja panosti uhkatilannekuvan ylläpitoon. Merkittävimmät erot liittyivät raportointikäytäntöihin ja teknisten häiriöiden käsittelyyn. Traficom painotti laajaa raportointia, mukaan lukien tekniset viat, kun taas Väylävirasto ja Fintraffic pyrkivät kevyempiin malleihin, jotka vähentävät resurssitarvetta. Lisäksi Fintraffic oli ainoa toimija, joka mainitsi systemaattisen uhkatilannekuvan kehittämisen tavoitteena. Yhteistyö eri toimijoiden välillä nähtiin kaikkien osapuolten kesken parantuneena, mutta turvaluokiteltujen tietojen jakaminen EU-tasolla jäi haasteeksi.

6 Johtopäätökset

Haastattelujen tuloksista voidaan päätellä, että NIS2-direktiivin tavoitteet ja raideliikenteen nykyiset käytännöt kohtaavat osittain, mutta niiden välillä on yhä selkeitä kehityskohteita. Tietoperusta alleviivasi yhtenäisten kyberturvallisuuskäytäntöjen tarvetta kansallisesti ja kansainvälisesti, riskienhallinnan keskeisyyttä ja valvontajärjestelmien tehokkuutta. Analyysin tulokset vahvistavat, että riskienhallinnan merkitys ymmärretään laajasti kaikissa tarkastelluissa organisaatioissa. Väylävirasto hyödyntää jo olemassa olevia viitekehyksiä, kuten ISO27001-standardia, mikä oli jo valmiiksi linjassa direktiivin vaatimusten kanssa. Traficom korostaa sääntelyn ja raportoinnin yhtenäistämistä, mikä puolestaan heijastaa NIS2 keskeisiä periaatteita.

Fintrafficin kohdalla turvallisuuskulttuurin muutos ja vanhojen teknologioiden päivittäminen osoittautuvat merkittäviksi haasteiksi, mikä antaa osviittaa siihen, että direktiivin asettamien teknisten vaatimusten täyttäminen on edelleen osittain puutteellista. Lisäksi poikkeamien raportointivaatimukset, erityisesti teknisten häiriöiden osalta, kielivät siitä, että EU

jäsenvaltioiden välisiä käytäntöjä tulisi yhä tasapäistää. Tietoperustan perusteella tiedonvaihdon ja yhteistyön tärkeys korostuu, mutta haastattelujen perusteella turvaluokiteltujen tietojen käsittelyssä koetaan edelleen haasteita, erityisesti jäsenmaiden välisessä tiedonvaihdossa.

6.1 Kehittämis- ja jatkotoimenpide-ehdotukset

Opinnäytetyön prosessissa syntyneen aineiston perusteella Suomen raideliikenteen kyberturvallisuuteen liittyen havaitut kehittämisehdotukset on esitetty taulukossa 4.

Toimenpide-ehdotus	Perustelu
Tiedon tavoitettavuuden yhtenäistäminen.	Kansalliset toimijat tulisi pysyväisluonteisesti määritellä ja auktorisoida siten, että turvaluokitellun tiedon luovuttamiselle ei olisi jatkossa lainsäädännöllistä estettä. Tällä saavutettaisiin yhä tiiviimpi yhtenäinen rintama toimijoiden kesken, joka mahdollistaisi yhä tehokkaamman yhtenäisen kyberturvallisuustoimijan Suomen raideliikenteen suojaamiseksi.
Selkeiden ja yhtenäisten kansallisten ja EU-tasoisten ohjeistusten laatiminen NIS2:n tulkintaan	Yhtenäiset ohjeet helpottaisivat poikkeamien raportointia, erityisesti teknisten häiriöiden osalta. Myös jäsenmaiden välinen raportointi ja tiedonvaihto muuttuisivat tasalaatuisemmaksi ja yhdenmukaisemmaksi.
Raideliikenteen kyberturvallisuuden asiantuntijoiden koulutus	Koulutetaan henkilöstöä raideliikenteen kyberturvallisuuden osaajiksi tulevaisuuden työvoimapulan ehkäisemiseksi. Yhteistyötä akateemisten ja koulutuksellisten tahojen kanssa tulisi tiivistää, jotta osaajapulaa voitaisiin tehokkaasti lieventää.
Teknologisten ratkaisujen modernisointi	Panostetaan teknologisten ratkaisujen modernisointiin siten, ettei toimijoille syntyisi enää tarvetta kompensoida puutteita riskienhallinnalla. Riskienhallinta on tehokas

	keino, mutta ei kuitenkaan korvaa täysin modernin tason teknologisia ratkaisuja ja täten yllä NIS2 vaatimusten tasolle.
Turvallisten tiedonvaihtokanavien perustaminen	Perustetaan kansallisia ja kansainvälisiä asiantuntijaryhmiä, joissa voidaan jakaa tietoa turvallisesti. Erityisesti turvaluokiteltujen tietojen käsittelyn tulisi näissä yhteistyöryhmissä olla sallittua ja avointa, jotta eri toimijoiden ja EU jäsenmaiden välisten toimintamallien ja havaintojen jakaminen tulisi aidosti mahdolliseksi.
Raportointiprosessien standardointi	Standardoidaan poikkeamien raportointiprosesseja mahdollisimman yksinkertaiselle ja käyttäjäystävälliselle tasolle, jotta raportoinnin aikataulupaineita voidaan todellisesti noudattaa myös viikonloppuisin ja loma-aikoina. Standardoidaan raportointiprosessit myös kansainvälisesti, jolloin reaaliaikainen uhkatilanneraportointi tulisi mahdolliseksi myös jäsenmaiden kesken.

Taulukko 4: Työn tulosten perusteella syntyneet kehittämisehdotukset

6.2 Pohdinta

Opinnäytetyön tavoitteena oli selvittää, mitkä ovat NIS2-direktiivin vaikutukset Suomen raideliikenteen kyberturvallisuudelle. Haastattelujen ja lähdemateriaalin avulla muodostettiin kuva NIS2-direktiivistä, sen sisällöstä ja velvoitteista sekä siitä, mitä toimenpiteitä se on aiheuttanut suomalaisissa raideliikenteen kyberturvallisuuteen liittyvissä keskeisissä organisaatioissa. Työn aineisto muodostui asiantuntijoiden haastatteluista, tutkimuskirjallisuudesta sekä muista luotettavaksi arvioiduista sähköisistä lähteistä, kuten erilaiset viranomaislähteet. Työn tuloksena syntyi myös konkreettisia toimenpide- ja kehitysehdotuksia. Tutkimusprosessi haastatteluineen oli mielenkiintoinen ja tarjosi kirjoittajalle uusia näkökulmia kriittisen infrastruktuurin kyberturvallisuuteen.

Opinnäytetyön tarkoituksena oli myös tuottaa tietoa työn tilaajalle, Laurea Ammattikorkeakoululle. Laurea tilasi opinnäytetyön tuottamaan tietoa spesifisti logistiikka-alan koulutusohjelmaa varten. Työn tuloksena tuotettiinkin lopulta ennalta arvaamattoman tärkeää tietoa, sillä tulosten pohjalta voidaan luotettavasti todeta, että Suomessa on nyt ja tulevaisuudessa

pulaa raideliikenteen kyberturvallisuuden osaajista. Laurea Ammattikorkeakoulu on tällä hetkellä sekä kansallisesti että kansainvälisesti arvostettu oppilaitos, jonka nykyinen kapasiteetti kyberturvallisuuden ammattilaisten kouluttajana on huippuluokkaa. Tilaajalla onkin kaikki potentiaali lähteä tutkimustyön tulosten pohjalta räätälöimään nykyistä kyberturvallisuuden koulutusohjelmaa nimenomaisesti raideliikenteen kyberturvallisuuden osaajapulaa ajatellen. Yhteistyössä raideliikenteen eri toimijoiden kanssa Laurea Ammattikorkeakoululla on mahdollisuus toteuttaa Suomen ensimmäinen raideliikenteen kyberturvallisuuteen erikoistuva kyberturvallisuuden koulutusohjelma. Koulutusohjelman pohjana voisivat toimia nykyiset kyberturvallisuuden laadukkaat perusopinnot, mutta erikoistumisopinnot ja työharjoittelut voisivat suuntautua suoraan raideliikenteeseen. Koulutusohjelman suunnittelussa ja toteutuksessa yhteistyökumppaneina voisivat toimia esimerkiksi opinnäytetyössä asiantuntijaorganisaatioina tunnetut Väylävirasto, Traficomin ja Fintraffic.

Kriittisen infrastruktuurin toimintakyky on jokaisessa modernissa valtiossa digitalisaation varassa. Digitalisaation myötä koko kriittisen infrastruktuurin kenttä on rampautettavissa kyberheikkouksia hyödyntäen. Kybermaailma on jatkuvassa muutoksessa, ja tässä muutoksessa puolustautujat ovat valitettavasti yleensä aina askeleen jäljessä. Syntyy uusia tekotapoja, uusia ilmiöitä, uusia keinoja ja ideoita vahingoittaa valtioiden toimintakykyä mitä monimuotoisemmin. Tämän negatiivisen muutoksen perässä Euroopan Unionin on kyettävä säännöllisesti päivittämään kyberturvallisuusdirektiiviään pitääkseen jäsenvaltionsa valppaina ja varautuneina. Direktiivin vaatimusten toteuttaminen aiheuttaa jäsenvaltioille hetkellisesti taloudellista taakkaa mm. lisäresurssitarpeiden ja teknologian modernisoinnin myötä, mutta samalla investoidaan kansalaisten turvallisuuteen. Samoin direktiivin vaatimusten jalkauttaminen käytäntöön aiheuttaa eri toimijoiden välisten johtosuhteiden ja velvollisuuksien uudelleenmäärittelyä ja prosessien muovaamista, mutta tämä olisi välttämätöntä ilman unionin ohjaustakin.

Kriittisen infrastruktuurin kyberturvallisuuden suojaamisessa ja ongelmiin varautumisessa jokaisen toimijan on oltava liitoksissa toisiinsa, ja jokaisella jäsenvaltiolla on oltava valmius toimia toistensa hyväksi. Siinä missä Suomen sotilaallinen puolustus on liitetty osaksi Natoa, on Suomen kyberturvallisuuden puolustus liitetty NIS2-direktiivin myötä yhä yhteneväisemmäksi osaksi Euroopan Unionia. Tämän opinnäytetyön havaintojen perusteella totean, että NIS-direktiivin päivityksen syvin olemus oli tuoda jäsenvaltiot yhä lähemmäs toisiaan kyberturvallisuuden saralla, ja täten muodostaa Euroopan Unionista yhä yhtenäisempi rintama.

Lähteet

Cisco. 2024. What is cybersecurity. Viitattu 23.1.2025. https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html#tabs-35d568e0ff-item-194f491212-tab

Enisa. 2020. Security measures in the railway transport sector. https://www.enisa.europa.eu/publications/railway-cybersecurity

Eskola, J. & Suoranta, J. 1998. Johdatus laadulliseen tutkimukseen. Tampere: Vastapaino

European Commission. 2024. Cybersecurity Policies. Viitattu 23.1.2025. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

Euroopan parlamentin ja neuvoston direktiivi (NIS2) 2022/2555/EU (32022L2555); EUVL L 333/80, 27.12.2022. Viitattu 29.8.2024. https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=fi

Euroopan komission suositus mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä (32003H0361); 2003/361/EY, EUVL L 124, 20.5.2003. Viitattu 29.8.2024. https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32003H0361

Graigen, D., Diakun-Thibault, N. & Purse, R. 2014. Defining Cybersecurity. Technology Innovation Management Review. 4,10. 13–21. Viitattu 30.1.2025. https://www.researchgate.net/publication/326309769_Defining_Cybersecurity

Ibadah, N., Benavente-Peces, C. & Pahl, M. 2024. Securing the Future of Railway Systems: A Comprehensive Cybersecurity Strategy for Critical On-Board and track-Side Infrastructure. Sensors 2024, 24(24), 8218. **https://doi.org/10.3390/s24248218** Viitattu 30.1.2025.

Traficom. 2024a. Raideliikenteen kyberturvallisuus. Viitattu 23.1.2025. https://www.traficom.fi/fi/liikenne/raideliikenne/raideliikenteen-kyberturvallisuus?toggle=Suositus%20kyberturvallisuuden%20edist%C3%A4misest%C3%A4%20raideliikenteess%C3%A4&toggle=Traficomin%20raideliikenteen%20palvelukokonaisuus&toggle=Traficomin%20Kyberturvallisuuskeskus

Traficom. 2024b. Rautatiesektorin toimijat. Viitattu 30.1.2025. https://www.traficom.fi/fi/liikenne/raideliikenne/rautatiesektorin-toimijat