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

Jyri Rajamäki and Tiina Kyrö
Laurea University of Applied Sciences, Espoo, Finland

Jyri.Rajamaki@laurea.fi
Tiina.Kyro@student.laurea.fi

Abstract: Sharing threat intelligence among stakeholders is crucial for a coordinated response to cyber threats. The updated cybersecurity directive of the European Union (NIS2) promotes collaboration and information sharing to strengthen cybersecurity across critical sectors, including transportation. This paper aims to examine how the NIS2 Directive has influenced the cybersecurity of Finland's transportation sector. Qualitative methods, including a literature review, semi-structured interviews, and thematic and comparative analyses, were employed. The study focuses on the perspectives of key Finnish railway cybersecurity actors regarding the impact of the NIS2 directive and current practices. The results reveal variations in the implementation challenges and strengths among organizations, with a unanimous emphasis on risk management. Development suggestions include standardizing incident reporting processes, creating uniform guidelines, increasing cybersecurity expertise, and enhancing collaboration among national actors.

Keywords: Cybersecurity, Transportation, NIS2 directive, DYNAMO project

1. Introduction

Cybersecurity has emerged as a critical concern in the global digital environment, where critical infrastructures are increasingly vulnerable to cyber threats. The European Union's NIS2 Directive (Network and Information Systems Directive) aims to strengthen cybersecurity and resilience in the critical sectors of member states, including transportation. This study, conducted in the context of the DYNAMO project, examines the impact of the NIS2 Directive on the cybersecurity of Finland's transportation sector, particularly railway systems. The study assesses how well Finland's transportation sector meets the requirements of the NIS2 Directive and identifies key challenges and opportunities for improving cybersecurity. The ultimate purpose of the study is to provide information on how DYNAMO tools can help meet the requirements of the NIS2 Directive.

The DYNAMO project focuses on enhancing the resilience of critical sectors such as energy, healthcare, and transportation by integrating Business Continuity Management (BCM) and Cyber Threat Intelligence (CTI) into a unified solution. The project's objective is to develop a platform, as depicted in Figure 1, that facilitates situational awareness for decision-making across all phases of the resilience management lifecycle (prepare, prevent, protect, respond, recover). (DYNAMO 2025)

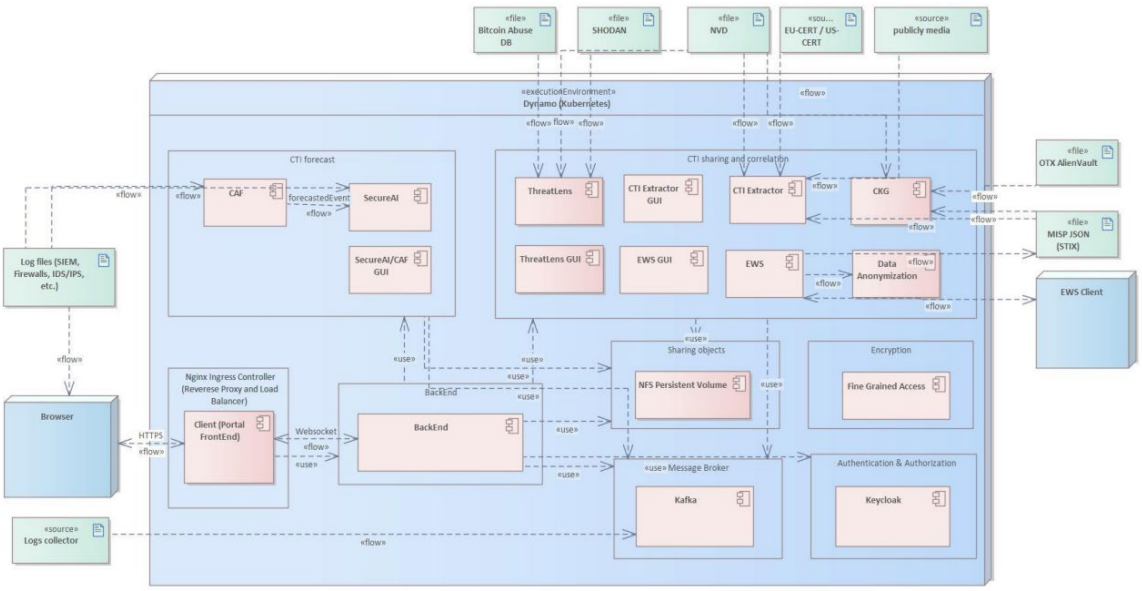

Figure 1: The DYNAMO platform (Chalkias, et al. 2024)

The DYNAMO platform combines Software as a Service (SaaS) and on-premises application models, providing situational awareness and supporting decision-making in risk scenarios (Chalkias, et al. 2024). The portal offers

access to the graphical user interfaces (GUI) of BCM/CTI components through a common view and Single Sign-On (SSO) via Keycloak[1], enabling in-depth analysis of CTI and BCM information. The communication between CTI and BCM components is ensured by web services and the Kafka[2] publish-subscribe pattern, which handles high-velocity, high-volume, and fault-tolerant data streams. The platform is deployed in a Kubernetes[3] environment, ensuring scalability and high availability. (Chalkias, et al. 2024)

The CTI framework provides threat detection and forecasting, correlation with relevant CTI data, and sharing with external entities after the anonymization of information by the Data Anonymization Tool (DAT). The SecureAI and Cyber Attack Forecasting (CAF) components perform threat detection and forecasting, and the data is pushed to the client's GUI for visualization. Users can choose to share the data with external entities via E-EWS and/or Malware Information Sharing Platform (MISP) or analyze the correlation using components such as ThreatLens, CTI Extractor, Cyber Knowledge Graph (CKG), or a combination thereof. CTI information is shared via a message broker with the BCM framework, which generates attack paths, risk and impact scenarios, and mitigation plans, and pushes them to the client GUI. (Chalkias, et al. 2024)

The deployment of the DYNAMO platform must consider legislative developments, and all parties must carefully study the applicable laws to ensure compliance with their obligations. This includes close collaboration between technology providers, end-users, and legal experts. The current EU legislative framework for digital products is based on Article 114 of the TFEU and includes various laws on specific products, safety aspects, and general product liability (Melenikou, 2024).

This paper complements the research by Rajamäki et al. (2024), which addresses the impact of the NIS2 directive on DYNAMO in the healthcare sector. The railways sector was chosen as the subject of this study also because it allows the lessons learned from the SAFETY4RAILS project (EOS, 2023) to be utilized in the DYNAMO project.

The study's central research questions are:

- How well does Finland's railway sector meet the technical and organizational requirements of the NIS2 Directive, and what are the key challenges and opportunities for improving cybersecurity?
- How can the DYNAMO platform and tools support the improvement of cybersecurity in the transportation sector and the fulfillment of the NIS2 requirements?

After this introduction, the methods section describes the data collection and analysis processes, detailing the selection of interviewees and the themes covered. The literature review provides an overview of the NIS2 Directive, its scope, and requirements, and discusses the cybersecurity challenges in Finland's transportation sector, particularly in railway systems. The results section summarizes the interview findings, highlighting the central role of risk management and common challenges such as the shortage of skilled personnel and handling classified information. The discussion emphasizes the need for technological modernization, standardized guidelines, and improved collaboration among stakeholders, while the conclusions summarize the key findings and underscore the importance of unified cybersecurity practices, risk management, and efficient monitoring systems.

2. Methods

This study employs a literature review, semi-structured interviews, thematic analysis, and comparative analysis. The objective is to analyse the impact of the NIS2 Directive on the cybersecurity of Finland's railway sector using interview data and a theoretical framework. The research methods were chosen to support qualitative analysis, focusing on thematic comparison and the differences and similarities in organizational perspectives. The study relies on qualitative methods because it examines experts' in-depth views and experiences regarding the implementation of the NIS2 Directive. Qualitative methodology provides a rich and detailed understanding of how the NIS2 directive is being implemented in the Finnish railway sector. Rather than quantifying compliance levels or applying a scoring model, the goal is to explore how cybersecurity professionals interpret and navigate regulatory changes in their specific organizational contexts. The use of semi-structured interviews and thematic

[1] https://www.keycloak.org/

[2] https://kafka.apache.org/

[3] https://kubernetes.io/

analysis enables the identification of underlying challenges, good practices, and development needs that would likely be overlooked by more quantitative approaches.

2.1 Selection of the Research Sample

The organizations for this study were selected through purposive sampling due to their critical and complementary roles in the governance, infrastructure, and operation of the national railway system. The aim was to capture diverse perspectives on the implementation of the NIS2 Directive from the regulatory, infrastructural, and operational levels. Their perspectives provided a comprehensive view of the NIS2 directive's impacts at different operational levels: regulation, infrastructure, and operational activities.

The following selected organizations represent Finland's railway cybersecurity landscape:

- Traficom (Finnish Transport and Communications Agency) is responsible for licensing, registration, and safety in transport and communications in Finland. It oversees and promotes transport and communications markets and services, ensuring the functionality and safety of communication networks and transport systems. Traficom serves as the regulatory authority for cybersecurity, tasked with developing and reporting on NIS2 Directive regulations. As the national authority, Traficom is responsible for regulating and supervising cybersecurity, as well as coordinating the implementation of the NIS2 Directive in Finland.
- The Finnish Transport Infrastructure Agency (Väylävirasto) is responsible for the development and maintenance of the state road network, railways, and waterways. It ensures the level of service in transport and participates in the coordination of transport and land use. Väylävirasto orders traffic control services from Fintraffic and collaborates with other authorities playing a significant role in cybersecurity management.
- Fintraffic provides and develops traffic control and management services for all modes of transport (road, rail, maritime, and air). It ensures the safety and smooth flow of traffic and offers real-time traffic information and digital services to businesses and consumers. Fintraffic is responsible for operational safety in collaboration with Traficom. Fintraffic handles real-time railway operations and cyber incident response. Together, these organizations provide a well-rounded understanding of how NIS2 is interpreted and implemented across governance, infrastructure, and operational domains.

2.2 Data Collection

Empirical data was collected through semi-structured interviews. The interviews were conducted remotely in October 2024, each lasting approximately one hour. The interview questions were sent to the interviewees approximately one week before the scheduled interview time. The interviews covered the following five themes:

- Practical implementation of NIS2 requirements
- Monitoring systems and reporting obligations
- Challenges and development needs
- Collaboration and stakeholders
- Management of cybersecurity threats

Notes were taken during the interviews and reviewed with the interviewees afterward to ensure accuracy and shared understanding. This verification process strengthened the reliability and transparency of the data. The review also encompassed ethical considerations, such as ensuring the confidentiality of interview data and avoiding the disclosure of detailed vulnerabilities that could compromise the security of Finland's transportation infrastructure.

2.3 Data Analysis

The collected data were analysed by using thematic analysis. The method was selected for its suitability in identifying and organizing patterns within qualitative interview data. The interview responses were organized under predefined five themes. These themes structured the data so that the perspectives of different organizations could be systematically compared after the interviews. The comparison identified clear common concepts and observations based on the impact of the NIS2 Directive from each interviewee's perspective.

The thematic framework enabled systematic comparison across the three organizations. The comparative analysis examined the similarities and differences in the themes that emerged during the interviews between organizations. Particular attention was paid to how different organizations have prepared for the directive's requirements, their reporting practices, and identified problem areas. The analysis revealed both shared

concerns and distinct organizational approaches, offering a comprehensive picture of how NIS2 implementation is progressing in the Finnish railway sector.

3. Literature Review

The literature review provides an overview of the NIS2 Directive, its scope, and requirements, and discusses the cybersecurity challenges in Finland's transportation sector, particularly in railway systems. In addition to EU-level documents and research project reports, this study draws from national-level strategies and regulatory frameworks that form the practical foundation of cybersecurity implementation in Finland. Key national documents include the Finnish National Cyber Security Strategy 2019 (Traficom), Traficom's sector-specific guidance, and ENISA reports. ISO/IEC 27001 standards were also referenced, as they have been integrated into several Finnish railway organizations. These sources help contextualize how EU-level regulation is translated into national and sector-specific action.

3.1 NIS2 Directive

The NIS directives, or the European Union's cybersecurity directives, were established to enhance the cybersecurity capabilities of the entire European Union, thereby supporting the overall security, economy, and societal functions of the union. The first directive, NIS1 (EU 2016/1148), which came into effect in 2016, significantly improved the union's cyber resilience by setting strategies for network and information systems security for member states and implementing uniform regulatory measures. However, a review revealed that, in addition to positive impacts, there were negative effects due to differences in national implementation among member states (Vandezande, 2023). Cybersecurity requirements varied significantly between member states, and in some cases, were even contradictory. These national differences in the implementation of the NIS directive caused fragmentation of the EU internal market and negatively affected cross-border service provision and the overall level of cyber resilience across the union. The updated NIS2 directive (EU 2022/2555), which came into effect in 2024, aims to eliminate these differences by strengthening minimum rules for the regulatory framework, enhancing cooperation arrangements among national competent authorities, updating the list of sectors and activities subject to cybersecurity obligations, and establishing effective legal remedies and enforcement measures essential for the effective implementation of obligations. (Schmitz-Berndt & Chiara, 2022)

3.1.1 Scope of the NIS2 directive

NIS2 establishes a cybersecurity regulatory framework that mandates European Union Member States to enhance their cybersecurity capabilities and risk management measures (Schmitz-Berndt, 2023). The NIS2 directive applies to both private and public entities that meet the criteria for medium-sized enterprises as defined in Recommendation 2003/361/EC or exceed the thresholds set for medium-sized enterprises. Medium-sized enterprises are defined as those with fewer than 250 employees and an annual turnover not exceeding 50 million euros or a balance sheet total not exceeding 43 million euros. Larger entities are those that exceed these criteria. The directive categorizes entities into two groups: essential and important entities.

3.1.2 Essential entities

Essential entities include those in highly critical sectors such as energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, ICT service management, public administration, and space. Additionally, essential entities include trust service providers, domain name registries, and DNS service providers regardless of their size, as well as providers of public electronic communications networks or services that meet or exceed the definition of a medium-sized enterprise. Public administration entities defined by national law as central or regional public administration entities whose disruption could significantly impact critical societal or economic functions are also included. Member states have the discretion to designate as essential entities those that provide critical services essential for the functioning of society or the economy, where disruption could have significant impacts on public order, safety, or public health, or cause significant systemic risk, especially in sectors with cross-border impacts. (Vandezande, 2023)

3.1.3 Important entities

Important entities include other critical sectors such as postal and courier services, waste management, chemicals manufacturing, production and distribution, food production, processing and distribution, manufacturing services, digital service providers, and research activities. Important entities also include highly

critical sectors that do not meet the definition of a medium-sized enterprise. Member states can designate as important entities those that provide critical services essential for the functioning of society or the economy, where disruption could have significant impacts on public order, safety, or public health, or cause significant systemic risk, especially in sectors with cross-border impacts.

3.1.4 Requirements for member states

The NIS2 directive imposes several requirements on member states to harmonize the level of cybersecurity and eliminate discrepancies. Each member state must adopt a national cybersecurity strategy that sets strategic objectives, the resources needed to achieve those objectives, and appropriate policy and regulatory measures to achieve and maintain a high level of cybersecurity. Member states must also regularly audit and update their national cybersecurity strategies at least every five years. Each member state must designate or establish one or more competent authorities responsible for cybersecurity and overseeing the implementation of the directive at the national level. A central contact point must also be designated or established. If a member state designates only one competent authority, it also serves as the central contact point. Member states must ensure that their competent authorities and central contact points have sufficient resources to effectively and efficiently fulfill their tasks and achieve the objectives of the NIS2 directive.

Each member state must designate or establish one or more cyber crisis management authorities responsible for managing large-scale cybersecurity incidents and crises. Member states must identify the capabilities, resources, and procedures that can be used in crisis situations and develop a national plan for managing large-scale cybersecurity incidents and crises. Each member state must also establish or designate one or more Computer Security Incident Response Teams (CSIRTs) responsible for monitoring and analyzing cyber threats, vulnerabilities, and incidents at the national level, responding to cybersecurity incidents, maintaining a cybersecurity situational picture, and issuing early warnings and alerts to essential and important entities and other relevant stakeholders. (Schmitz-Berndt & Chiara, 2022)

3.1.5 Requirements for entities

The NIS2 directive requires member states to ensure that essential and important entities implement appropriate and proportionate technical, operational, and organizational measures to manage risks to the security of network and information systems used in their operations or service provision and to prevent or minimize the impact of incidents on service recipients and other services. The proportionality of measures must consider the extent to which the entity is exposed to risks, its size, and the likelihood and severity of incidents, including their societal and economic impacts. The directive also establishes different supervisory regimes for essential and important entities. Essential entities are subject to comprehensive supervision, including both ex-ante and ex-post supervision, while important entities are subject to lighter supervision, including only ex-post supervision. The two-tier supervisory regime aims to ensure a fair balance of obligations between entities and competent authorities.

The directive sets minimum requirements for measures, including risk analysis and information system security policies, incident handling, business continuity management, supply chain security, security of network and information systems acquisition, development, and maintenance, assessment of the effectiveness of cybersecurity risk management measures, basic cyber hygiene practices and cybersecurity training, cryptography and encryption policies, personnel security, access management policies, and the use of multi-factor authentication or continuous authentication solutions, secure communication systems, and secure emergency communication systems.

The NIS2 directive also imposes reporting obligations on essential and important entities for significant incidents. Incidents must be reported without undue delay to the CSIRT or the competent authority. An incident is considered significant if it has caused or could cause severe operational disruption or financial losses to the entity, or if it has affected or could affect other natural or legal persons by causing substantial material or non-material damage. Entities must report an early warning within 24 hours of becoming aware of the incident, indicating whether it is suspected to be caused by unlawful or hostile acts or could have cross-border impacts. A subsequent incident report must be submitted within 72 hours, detailing the severity and impact of the incident, and a final report must be submitted within one month.

National cybersecurity authorities are required to assess compliance with the obligations of the NIS2 Directive, and various assessment frameworks have been developed for this purpose. For example, Divas et al. (2020) describe a Cybersecurity Maturity Assessment Framework (CMAF), which can be used either as a self-assessment tool for operators of essential services and digital service providers or as an audit tool for national

cybersecurity authorities. According to Ferguson (2023), cybersecurity risk management measures of the NIS 2 Directive may be limited in preventing cyberattacks, because they focus more on mitigating the impact rather than preventing attacks, allowing serious and persistent effects on essential and important entities. Threat actors can progress through early attack phases with minimal hindrance, achieving significant impacts. Information superiority during the reconnaissance phase is crucial, and additional measures like vulnerability scanning and penetration testing are recommended, though not explicitly required by the directive (Ferguson, 2023).

3.2 Cybersecurity of the Finnish Transportation Sector

The importance of cybersecurity in the transportation and logistics sector has significantly increased with digitalization (Leviäkangas, 2016). The major impacts on the logistics sector are:

- Operational Disruptions: Cyberattacks can cause significant disruptions in the logistics chain, such as delivery delays and operational interruptions.
- Financial Losses: Attacks, such as ransomware, can lead to substantial financial losses as companies may have to pay ransoms or repair damages.
- Data Breaches: Logistics companies handle large amounts of sensitive information, such as customer data and delivery schedules. Leaks of this information can cause reputational damage and legal consequences.
- Regulatory Compliance: Companies must adhere to strict cybersecurity regulations and standards, which require continuous monitoring and investments.

The transportation sector in Finland consists of several key modes of transport (Leviäkangas, 2016):

- Road Transport: This is the largest segment, accounting for about 90% of domestic freight transport.
- Water Transport: A significant portion of international freight is transported via waterways, especially through maritime shipping.
- Rail Transport: Railways play a crucial role, particularly in the transportation of heavy goods. Rail transport provides direct connections to ports, enabling efficient transfer of goods between ships and trains. This reduces transportation time and costs.
- Air Transport: Although its share in terms of tonnage is small, air transport is vital for high-value and urgent shipments.

In the next, we will conduct a more detailed examination of railway transportation cybersecurity, and the insights gained from the SAFETY4RAILS project (EOS, 2023; Bonneau, et al., 2022).

3.3 Railway Cybersecurity

Railway systems largely consist of various sensors and electronic devices designed to monitor operations and enable remote supervision. These electronic devices on the tracks are interconnected and linked to sensors on trains. Both types of sensors are crucial for ensuring the safety and real-time monitoring of railway operations. Train sensors collect and transmit data on train performance, track conditions, and the surrounding environment, while track sensors gather information on the environment, track physical conditions, and trains. Sensors are categorized based on their functions, such as safety monitoring sensors, environmental sensors, and train performance sensors. Technological advancements in railways have improved efficiency and safety, but have also introduced cybersecurity challenges (Bonneau, et al., 2022).

Railway cybersecurity faces risks that can potentially harm the physical world, railway safety, and operational reliability. The primary task of various stakeholders in the railway system is to identify and manage these risks, as cybersecurity is now recognized as an integral part of overall railway safety (Crabbe, et al., 2022). in Finland, Traficom is responsible for developing and coordinating railway cybersecurity, preventing cybersecurity breaches, disseminating information on cybersecurity issues, and investigating breaches and threats. Traficom serves as the national cybersecurity centre.

Examples of Cyber Attacks on Railways Worldwide (Crabbe, et al. 2022):

- October 2017, Sweden: Two denial-of-service (DoS) attacks targeted the Swedish Transport Administration (Trafikverket) through its two internet service providers. The first attack disrupted the train location service, email system, website, and traffic maps, forcing manual reservation systems to be used. The second attack affected the website of the Swedish Transport Administration and the

public transport operator Vasttrafik in Western Sweden, causing the ticketing app and online travel planning service to crash.

- May 2018, Denmark: A DoS attack impacted the railway ticketing systems, preventing Danish passengers from purchasing tickets from ticket machines, online applications, websites, or certain station kiosks. Approximately 15,000 customers were affected.
- March 2020, United Kingdom: A data breach exposed customer information from free Wi-Fi services at railway stations. Around 10,000 email addresses and travel details of users were leaked online. Network Rail and service provider C3UK confirmed the incident, which involved a database containing 146 million records, including personal contact details and birthdates. The breach also affected the "Indian Rail" app, popular on Apple's App Store, due to an exposed Firebase database containing over 2.3 million rows of emails, usernames, and plaintext passwords.

4. Results

This section provides a detailed analysis of the interview results and comparative analysis, highlighting the diverse impacts of the NIS2 Directive on the cybersecurity practices of different organizations within Finland's railway sector.

4.1 Interview Results

Based on the interviews, it was found that the impacts of the NIS2 Directive on the cybersecurity of Finland's railway sector vary depending on the organization. All interviewees emphasized the central role of risk management in meeting the directive's requirements, but the approaches and emphases differ. Traficom highlighted the lack of proactive oversight and stressed the operators' own responsibility for risk management. The Finnish Transport Infrastructure Agency (Väylävirasto), on the other hand, has integrated the NIS2 requirements into its existing processes, resulting in minimal additional workload. Fintraffic identified cultural change and updating old technology as its biggest challenges.

There were similarities in reporting practices: all entities use existing systems, but Traficom emphasizes the reporting of technical disruptions, which has sparked discussions within the EU. Additionally, the interviewees pointed out the shortage of skilled personnel and the challenges in handling classified information as significant obstacles to the implementation of the directive. A positive development noted was the strengthening of stakeholder collaboration, which has led to improved information exchange and joint cybersecurity exercises.

4.2 Comparative Analysis Results

The comparative analysis revealed clear similarities and differences among the organizations. All entities emphasized the importance of risk management and identified the shortage of skilled personnel as a challenge, but their readiness to meet NIS2 requirements varied. The Finnish Transport Infrastructure Agency (Väylävirasto) was the least dependent on the directive's guidelines, as its existing frameworks, such as ISO27001, are already aligned with the requirements. Traficom, on the other hand, focused particularly on regulatory development and comprehensive reporting, while Fintraffic emphasized collaboration with other stakeholders and invested in maintaining a threat landscape overview.

The most significant differences were related to reporting practices and the handling of technical disruptions. Traficom emphasized extensive reporting, including technical faults, whereas Väylävirasto and Fintraffic aimed for lighter models that reduce resource requirements. Additionally, Fintraffic was the only entity that mentioned the goal of systematically developing a threat landscape overview. Collaboration among different entities was seen as improved by all parties, but the sharing of classified information at the EU level remained a challenge.

5. Discussion

The technical requirements of the NIS2 Directive emphasize the standardization of network and information system security. For Finland's railway sector, this primarily means updating outdated railway technologies, as their vulnerabilities inevitably increase risks and complicate compliance with the directive's standards. Alongside technological modernization, the broader application of internationally recognized standards, such as ISO27001, is recommended. The literature review highlights the continuous development of technology to combat emerging cyber threats.

The NIS2 Directive also introduces organizational requirements, such as clearer delineation of responsibilities and more effective collaboration among different entities. This is particularly important in the transportation sector, where entities like Traficom, the Finnish Transport Infrastructure Agency (Väylävirasto), and Fintraffic

are interdependent. The directive emphasizes that successful cybersecurity efforts require effective coordination between organizations and the development of functional collaboration structures both nationally and internationally. Additionally, the ability of organizations to meet reporting requirements and manage incidents is crucial for the implementation of the directive.

This study found that there is still a need for improvement in handling classified information. This is particularly evident in both national and EU-level cooperation, as practices vary and there are legal barriers to information sharing. At the same time, the efficiency of information exchange and the maintenance of situational awareness were seen as critical factors in strengthening cybersecurity.

5.1 Action Proposal for Finnish Railway Sector

Based on the interviews, the development-oriented framework for improving NIS2 compliance in the railway sector in Finland, as presented in Table 1, was identified.

The framework includes standardizing incident reporting protocols to ensure timely responses even during weekends and holidays, creating secure and harmonized procedures for the handling of classified information, investing in the modernization of legacy technologies and addressing the cybersecurity talent gap. These recommendations reflect systemic needs in the Finnish railway sector and may offer transferable insights for other EU member states facing similar implementation challenges.

Table 1: Development Framework for NIS2 Compliance in the Finnish Railway Sector

Development Area	Description
Incident Reporting	Standardize protocols for timely response, including weekends and holidays
Classified Information Handling	Establish secure and harmonized procedures for sharing sensitive data
Legacy System Modernization	Invest in upgrading outdated technologies that pose security risks
Cybersecurity Talent	Address the skill gap by improving education and recruitment in the sector

5.2 Enhancing Cybersecurity Collaboration with DYNAMO

To strengthen collaboration among key national stakeholders, the accessibility of information must be standardized. National actors should be permanently defined and authorized so that there are no legal barriers to the transfer of classified information in the future. This will achieve a more cohesive and unified front among stakeholders, enabling a more effective and unified cybersecurity entity to protect Finland's railway sector. The DYNAMO project's emphasis on cyber-threat intelligence sharing and orchestration (Task 4.2) aligns with the recommendation for improved collaboration among national and international stakeholders. DYNAMO can facilitate secure and efficient information exchange, including the handling of classified information, which is crucial for coordinated cybersecurity efforts.

Clear and consistent national and EU-level guidelines should be established to mandate the uniform interpretation of NIS2 Directive requirements. Standardized guidelines will facilitate incident reporting, particularly for technical disruptions. Additionally, reporting and information exchange between member states would become more consistent and uniform. DYNAMO's focus on standardizing and simplifying incident reporting processes can directly address the recommendation for harmonized reporting practices. The integration of AI and machine learning can streamline the reporting of technical disruptions and ensure timely and accurate incident documentation.

Personnel should be trained as cybersecurity experts in railway transportation to prevent future workforce shortages. Collaboration with academic and educational institutions should be intensified to effectively mitigate the skills gap. DYNAMO can contribute to the recommendation for increasing cybersecurity expertise by developing training programs and resources. Collaboration with academic and educational institutions within the project can help address the skills gap and prepare a future workforce specialized in railway cybersecurity.

Investment in the modernization of technological solutions should be prioritized so that stakeholders no longer need to compensate for deficiencies with risk management. While risk management is an effective tool, it does not fully replace modern technological solutions and thus maintains compliance with NIS2 requirements. DYNAMO's focus on integrating cutting-edge technologies and modernizing existing systems can support the recommendation for technological upgrades. This would ensure that stakeholders have access to the latest tools and solutions to meet NIS2 requirements effectively.

National and international expert groups should be established to share information securely. In these collaborative groups, the handling of classified information should be allowed and open, enabling the genuine sharing of operational models and observations between different stakeholders and EU member states. By leveraging the advanced threat intelligence gathering and extraction capabilities developed in Task 4.1, DYNAMO can provide more comprehensive and up-to-date threat intelligence. This would improve the accuracy and relevance of the threat landscape overview for Finland's transportation sector.

Incident reporting processes should be standardized to the simplest and most user-friendly level possible, ensuring that reporting deadlines can be realistically met even on weekends and holidays. Reporting processes should also be standardized internationally, allowing real-time threat situation reporting between member states. The AI-driven analysis and correlation tools from Task 4.3 and predictive analytics from Task 4.4 can enhance the ability to foresee and mitigate potential cybersecurity threats. This would support the recommendation for continuous technological development and proactive risk management.

6. Conclusions

The findings of this study suggest that the objectives of the NIS2 Directive and the current practices in the transportation sector partially align, but there are still clear areas for improvement. The literature emphasizes the need for unified cybersecurity practices both nationally and internationally, the centrality of risk management, and the efficiency of monitoring systems. The analysis results confirm that the importance of risk management is widely understood across all examined organizations. The Finnish Transport Infrastructure Agency (Väylävirasto) already utilizes existing frameworks, such as the ISO27001 standard, which are aligned with the directive's requirements. Traficom emphasizes the harmonization of regulations and reporting, reflecting the core principles of NIS2. For Fintraffic, the challenges of cultural change and updating outdated technologies are significant, indicating that compliance with the directive's technical requirements is still partially lacking.

The literature underscores the importance of information exchange and collaboration, but the interviews reveal ongoing challenges in handling classified information, especially in the exchange of information between member states. The incident reporting requirements, particularly for technical disruptions, suggest that practices among EU member states need further harmonization. The findings also suggest that while some organizations have already made progress in NIS2-related areas, such as aligning with ISO27001, other recommendations—like talent development and legacy system modernization—will require sustained effort and long-term investment. These time horizons should be considered in national and EU-level implementation planning.

The DYNAMO platform and tools can support the improvement of cybersecurity in the transportation sector and the fulfillment of NIS2 requirements in the following ways: *(1) Standardizing Incident Reporting:* Simplifying and harmonizing incident reporting processes to ensure timely responses, even during weekends and holidays. *(2) Enhancing Information Sharing:* Facilitating secure and efficient information exchange, including the handling of classified information, to improve collaboration among national and international stakeholders. *(3) Modernizing Technology:* Integrating cutting-edge technologies and modernizing existing systems to meet NIS2 requirements effectively. *(4) Addressing Skill Gaps:* Developing training programs and resources to increase cybersecurity expertise and mitigate the skills gap in the sector. *(5) Improving Situational Awareness:* Providing tools for threat detection, forecasting, and maintaining a comprehensive threat landscape overview. These measures will help ensure a cohesive and effective approach to cybersecurity in the transportation sector.

Acknowledgements

Acknowledgment is paid to the DYNAMO Project, funded by the European Union under grant agreement no. 101069601. Views and opinions expressed are, however, those of the authors only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

References

Bonneau, M.-H., et al. (2022) “SAFETY4RAILS EU project: Protecting railway and metro infrastructure against combined cyber-physical attacks”, *World Congress on Railway Research (WCRR)*.

Chalkias, I., et al. (2024) “D4.1 Initial prototypes of the cyber-threat intelligence gathering, extraction, sharing components and AI-based solutions”, v2.0, DYNAMO, 18 October. Available: https://horizon-dynamo.eu/wp-content/uploads/2025/02/DYNAMO-RPT-D41-V2-0.pdf

Crabbe, S., et al. (2022) "SAFETY4RAILS Information System platform demonstration at Madrid Metro simulation exercise", *Proceedings of the 32nd European safety and reliability conference*.

Drivas, G., et al. (2020) "A NIS directive compliant cybersecurity maturity assessment framework", *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, pp 1641-1646.

DYNAMO (2025) "Home", [online] https://horizon-dynamo.eu/

ENISA (2023) *ENISA Threat Landscape 2923*, European Union Agency for Cybersecurity (ENISA). Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

EOS (2023) "SAFETY4RAILS (H2020 – GA Number: 883532)", [online] https://www.eos-eu.com/safety4rails

European Commission (2024) "Cybersecurity Policies", [online] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

European Parliament and Council (2022) "Directive (NIS2) 2022/2555/EU", [online] https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

Ferguson, D.D.S. (2023) "The outcome efficacy of the entity risk management requirements of the NIS 2 Directive", *Int. Cybersecur. Law Rev.* **4**, 371–386. Available: https://doi.org/10.1365/s43439-023-00097-8

ISO/IEC 27001:2022. "Information security, cybersecurity and privacy protection — Information security management systems — Requirements"

Leviäkangas, P. (2016) "Digitalisation of Finland's Transport Sector", *Technology in Society,* Vol. 47, pp. 1–15, doi:10.1016/j.techsoc.2016.07.001.

Melenikou, G., et al. (2024) "D1.3 Ethical and Legal Protocol and Compliance Assessment", DYNAMO, 27 March. Available: https://horizon-dynamo.eu/wp-content/uploads/2024/03/DYNAMO-D1.3-PU-M18.pdf

Rajamäki, J., et al. (2024) "Implications of GDPR and NIS2 for Cyber Threat Intelligence Exchange in Hospitals", *WSEAS Transactions on Computers,* Vol. 23, doi: 10.37394/23205.2024.23.1.

Schmitz-Berndt, S. (2023) "Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive", *Journal of Cybersecurity*, Vol. 9, Iss. 1, p. tyad009, https://doi.org/10.1093/cybsec/tyad009.

Schmitz-Berndt, S. and Chiara, P. G. (2022) "One Step Ahead: Mapping the Italian and German Cybersecurity Laws against the Proposal for a NIS2 Directive", *International Cybersecurity Law Review*, Vol. 3, No. 2, pp. 289–311, doi:10.1365/s43439-022-00058-7.

Vandezande, N. (2023) "Cybersecurity in the EU: How the NIS2-Directive Stacks up against Its Predecessor", *Computer Law & Security Review*, Vol. 52, pp. 105890–105890, doi:10.1016/j.clsr.2023.105890.