Cyber-resilient cross-border smart mobility between Moldova, Ukraine, and Romania: integrating AI and digital platforms for secure data management

Anatolie BABIN
Academy of Economic Studies of Moldova, Chisinau, Republic of Moldova
anatolii.babin@ase.md

Sergey SERDYUK
Deputy Chief of the State Border Service of Ukraine, Kyiv, Ukraine
adpsu@dpsu.gov.ua

Rafael CILOCI
Technical University of Moldova, Chisinau, Republic of Moldova
rafael.ciloci@fieb.utm.md

Annotation
The growing complexity of cross-border transport systems in Eastern Europe presents both opportunities and challenges for building cyber-resilient smart cities. Ensuring safe, efficient, and sustainable mobility between Moldova, Ukraine, and Romania requires innovative integration of digital platforms and artificial intelligence. Objectives:This study explores strategic approaches to development. cyber-resilient cross-border intelligent mobility systems in the region. It is aimed at proposal of a model using AI and digital platforms to optimize transport flows, improve data security, and support sustainable regional development in border areas.Previous research: The study draws on initiatives such as the Three Seas initiative, EIT Urban Mobility, the EIT Regional Innovation Scheme (RIS), and the Connect2SmallPorts digital audit platform. It also takes into account EU strategies, including the Sustainable and Smart Mobility Strategy, the Intelligent Transport Systems Directive, and the European Green Deal, as well as current research on digital, environmental, and social transformations for regional development. Approach: A mixed-method approach was used, combining institutional and policy analysis, cross-border case studies, and the evaluation of digital tools for transport monitoring and data integration. Methods include comparative diagnostics of traffic flows, AI-based traffic management and assessing cybersecurity and compliance measures. Results: AI-powered monitoring platforms and digital auditing ensure safe, efficient, and compatible cross-border transport management, reducing waiting times, minimizing environmental impacts, and improving cooperation between transport authorities. Regional innovation systems, digital clusters, and observatories are key factors for data-driven policymaking and the international integration of local economies.Conclusion: The study's findings are relevant for policymakers, transport authorities, urban planners, and researchers, promoting evidence-based decision-making and strengthening cross-border cooperation. Value: The study offers an interdisciplinary concept that combines AI, digital platforms and strategies for regional innovation to build cyber-resilient cross-border intelligent mobility, providing both academic and practical contributions.

Keywords: cross-border mobility, cybersecurity, artificial intelligence, digital platforms, regional innovation

1. Introduction
The cross-border transport system between Moldova, Ukraine, and Romania is facing increasing complexity due to increasing passenger and freight flows, geopolitical dynamics, and integration with European Union (EU) policies. In this context, ensuring cyber-resilient smart mobility is essential to improve efficiency, safety, and sustainability [1,2]. Moldova and Ukraine, as EU candidate countries, participate in initiatives such as the Three Seas Initiative and the Danube Strategy, which emphasize regional connectivity,

digitalization, and the sustainability of transport infrastructure [3]. Furthermore, European platforms such as the JRC (Joint Research Centre) provide research-based recommendations for the integration of AI and digital data into smart mobility systems [4].

This study focuses on the strategic integration of AI, digital platforms, and cybersecurity measures to ensure effective cross-border transport management. This includes the use of interoperable datasets (spatial, transport, environmental, and social data), as well as coordination mechanisms for national and transnational cybersecurity command centers (CSCs) in response to potential incidents [5].

A Spatial Data Infrastructure (SDI) [6] serves as a fundamental foundation for ensuring data interoperability in a cross-border context. At its core, an SDI is a structured system for collecting, storing, managing, and exchanging geospatial data between various stakeholders in a standardized manner. In the context of Moldova, Ukraine, and Romania, the SDI plays a crucial role in harmonizing information related to border management, transport corridors, traffic flows, and environmental conditions. By establishing standardized data formats and protocols, the SDI reduces vulnerabilities arising from inconsistent or incompatible systems. Furthermore, the use of clear metadata, access control, and secure APIs ensures the reliable and secure exchange of sensitive geospatial and transport data across borders. For example, real-time border traffic data transmitted via the Spatial Data Infrastructure (SDI) enables artificial intelligence-based systems to optimize vehicle flows while ensuring that only authorized entities have access to sensitive information. The adoption of national laws on spatial data infrastructure (SDI) in Moldova (2016) and Ukraine (2019) provides a legal and technical basis for harmonised geospatial data, enabling cross-border smart mobility and alignment with European transport and research networks.

2. Intelligent transport systems and digital platforms

Intelligent transport systems (ITS) [7] form the foundation of cyber-resilient smart mobility. ITS integrate AI-based predictive traffic management, digital monitoring platforms, and decision support tools to optimize passenger and freight flows . Key datasets include:

- Geospatial data: road networks, transport corridors, border crossing points;
- Transport details: Number of passengers, cargo flows, schedules;
- Environmental data: CO_2emissions, pollution levels;
- Social data: accessibility indicators, user reviews;
- IT and Cybersecurity Event Logs: network events, incident reports.

AI algorithms use these datasets to predict traffic peaks, optimize routes, and minimize environmental impacts. Valuable datasets, such as detailed geospatial maps and real-time border data, are crucial for cross-border interoperability, enabling the creation of regional observatories and digital twins of transport infrastructure. Digital platforms, including Connect2SmallPorts [8] , EIT Urban Mobility RIS [9], and the X4ITS [10] (Cross for ITS) initiative, enable real-time monitoring, data harmonization, interoperability of intelligent transport systems, and coordination between transport authorities across borders. These systems support the implementation of harmonized ITS and C-ITS services [11] on TEN-

T corridors [12] and multimodal transport nodes, while also providing secure access for stakeholders and ensuring compliance with EU data protection [13] and cybersecurity standards [14]. In Moldova, Ukraine, and Romania, the implementation of digital platforms for transport management and real-time monitoring is particularly relevant in areas with high passenger and freight traffic, as well as in border towns and transport corridors connecting the countries. This primarily applies to key border crossings such as Palanca (Moldova) - Reni (Ukraine), Soroca (Moldova) - Iasi (Romania), as well as transport hubs on highways included in Pan-European Corridors VIII and IX[15], which serve major freight routes and international bus lines.

Areas with a high concentration of port and river infrastructure, including small ports on the Dniester and Danube, also require the implementation of digital monitoring systems similar to the European Connect2SmallPorts platform, which integrates logistics flows and automated vessel and cargo tracking. In cities with intense intra-urban and suburban traffic, such as Chisinau, Odesa, and Iasi, the use of solutions like EIT Urban Mobility RIS allows for the optimization of public transport routes, the collection of passenger flow data, and real-time adjustments to transport systems. The use of these platforms not only ensures data harmonization and coordination between transport authorities across countries, but also secure access for stakeholders while complying with EU standards for personal data protection and cybersecurity. Therefore, the priority implementation of digital platforms should focus on:

1. Border crossings and transport corridors, where large international flows of passengers and cargo are formed;
2. Port and river hubs, providing international logistics;
3. Urban centers with high traffic density, where digital monitoring improves the efficiency and sustainability of the transport system.

To better demonstrate the spatial distribution of the proposed digital infrastructure, it is important to visualize the main priority zones where intelligent transport systems, AI-based monitoring platforms, and cybersecurity coordination mechanisms should be implemented first. These areas include strategic border crossings, international transport corridors, urban mobility hubs, and river-port infrastructure connecting Moldova, Ukraine, and Romania. The following figure 1, presents the priority of urban areas in the frontier regions, districts for deployment of smart mobility and digital monitoring platforms within the cross-border transport ecosystem.



Fig. 1. Some priorities areas for deployment of ITS in Moldova, Ukraine, and Romania
Source: created by the authors.

The EIT Urban Mobility RIS approach can be effectively adapted to the implementation of the X4ITS project practices in Moldova, Ukraine, and Romania, particularly in the context of fragmented ITS development, differing national implementation speeds, and the need for harmonized cross-border mobility solutions. Similar to X4ITS, the EIT Urban Mobility RIS framework promotes digital integration, innovation ecosystems, interoperable mobility services, and cooperation between public authorities, transport operators, research institutions, and technology providers. In the context of the Danube Region and Eastern Europe, where transport systems are characterized by linguistic diversity, heterogeneous infrastructure, and intensive cross-border mobility, the EIT Urban Mobility RIS model provides a practical basis for strengthening regional connectivity and data-driven transport governance. The adaptation of X4ITS practices through the EIT Urban Mobility RIS approach enables the creation of coordinated digital transport ecosystems connecting high-level TEN-T corridors, secondary road infrastructure, multimodal hubs, and urban mobility systems. Particular importance is given to the harmonization of ITS applications, the development of interoperable National Access Points (NAPs), and the implementation of AI-supported traffic management systems capable of processing real-time mobility data across borders. Such integration is especially relevant for Moldova and Ukraine as candidate countries seeking alignment with EU transport, cybersecurity, and digitalization standards.

Within this framework, the experience of the previous CROCODILE initiative [16] and the current X4ITS project demonstrates the importance of coordinated data exchange and standardized communication protocols for improving transport efficiency and mobility services. The EIT Urban Mobility RIS methodology complements these objectives by supporting innovation-driven urban mobility solutions, pilot testing environments, regional living labs, and collaborative governance mechanisms. This approach allows border regions and urban centers such as Chisinau, Odesa, Iași, and cross-border corridors including Palanca–Reni and Danube logistics routes to implement harmonized ITS and C-ITS services while ensuring cyber resilience and interoperability with European transport

systems. Furthermore, the combined application of X4ITS and EIT Urban Mobility RIS contributes to achieving broader European strategic priorities, including decarbonization, digital transformation, Vision Zero road safety objectives, and sustainable mobility development.

The integration of AI-based analytics, multimodal transport coordination, environmental monitoring, and cybersecurity platforms strengthens the resilience of cross-border transport infrastructure and improves the quality of mobility services for passengers and freight operators. As a result, this adapted approach creates favorable conditions for deeper integration of Moldova and Ukraine into the European mobility and digital ecosystem while supporting sustainable regional development in the Danube and Black Sea areas.

3. Cross-border coordination in the field of cybersecurity

Building a cyber-resilient mobility system requires robust coordination between national and transnational security operations centers (SOCs)[17]. In Moldova, Ukraine, and Romania, national SOOCs monitor and respond to security incidents, while cross-border cooperation ensures coordinated incident management and information sharing [5,10]. Typically, the operational procedure includes:

1. Anomaly detection using AI-based monitoring;
2. Reporting incidents to national emergency response centres;
3. Forwarding information to regional or European Computer Emergency Response Teams (CERTs) for cross-border review;
4. Sharing data with cross-regional platforms such as Smart Cyber Regions enables joint threat analysis, simulation exercises and protocol harmonization [18].

Integration into the cybersecurity framework of smart regions increases resilience by standardizing security procedures, enabling cross-border testing of solutions, and creating a shared knowledge base. This approach ensures that valuable transport and geospatial datasets remain secure, interoperable, and usable for AI analytics [19]. Fortai EU AI Act Compliance is a platform designed to ensure that AI development in Europe complies with the EU AI Act (2024/1689) [20]. New EU initiatives aim to simplify the transition to compliance with the AI Act for small and medium-sized enterprises. In the cross-border smart mobility sector, it helps ensure that digital transport algorithms, autonomous vehicle software, and machine learning models for traffic management (AI in Transportation - GeeksforGeeks) comply with strict transparency and risk ranking laws. To ensure effective compliance with the EU AI Act and to support secure deployment of AI-driven smart mobility solutions in cross-border environments, it is necessary to define the required technological capabilities of the underlying infrastructure. In particular, transport-related AI systems - such as predictive traffic management, anomaly detection, and autonomous decision-support tools - depend on a combination of computing power, secure communication channels, data storage capacity, and governance mechanisms for model deployment and monitoring. The following figure 2 presents a structured capability matrix of AI infrastructure components required for the implementation of cyber-resilient cross-border smart mobility systems.



Fig. 2. AI infrastructure capability matrix for cyber-resilient cross-border smart mobility system
Source: created by the authors.

As illustrated in the AI infrastructure capability matrix, the effective deployment of intelligent transport systems requires a layered architecture combining high-performance computing resources, secure and segmented communication networks, scalable data storage systems, and integrated AI orchestration tools. These components collectively ensure the secure processing of large-scale transport and geospatial datasets, enable real-time analytics for traffic optimization, and support automated threat detection and response. Moreover, the integration of cybersecurity monitoring tools such as FortiAI and FortiGate strengthens system resilience against cyber threats, while ensuring compliance with EU regulatory frameworks, including the EU AI Act. This architecture provides a foundation for scalable, interoperable, and secure AI deployment across Moldova, Ukraine, and Romania. In the local context, located at a crucial cross-border hub for Europe, Moldova and Ukraine is expanding its participation in the Digital Europe program, enabling organizations to leverage pan-European cybersecurity systems. As cross-border automated mobility corridors expand, tools like FortiAI are providing a foundation for preventing cyberattacks before they disrupt cross-border logistics and transportation.

1. Compliance with the EU AI Law

- Risk Mapping: The platform evaluates AI systems to classify them as prohibited, high-risk (e.g., critical transportation infrastructure), or limited-risk.
- Audit Ready: It generates downloadable PDF reports detailing whether your systems comply with Article 5, Annex III and Article 50 of the regulation, helping companies avoid large financial fines.
- Operational Transparency: It helps developers of cross-border routing, smart logistics, and autonomous delivery systems maintain the necessary transparency and risk management protocols. AI in Transportation [21]

2. Multi-country mobility data spaces in the EU [22]
- Data integration: The EU is investing heavily in creating a common European mobility data space to seamlessly exchange logistics and transport data in real time across borders.
- Standardised cooperation: Platforms must comply with European standards (e.g. DATEX II) for the exchange of real-time traffic and safety information between regional access points.

3. Smart Mobility Initiatives [23]
- Predictive management: AI in smart mobility uses real-time data to optimize vehicle routes, predict maintenance, and adjust traffic lights to reduce congestion. AI in Transportation.
- 5G Corridors: Cross-border corridors are being digitalised through EU research programmes to ensure seamless, interconnected transport from one Member State to another with the rollout of European 5G cross-border corridors [24].

Fortinet's FrontAI [25] solutions in franewors of innovative pulic private partnership [26] can play a critical role in cross-border intelligent mobility, providing automated, real-time protection for connected and autonomous vehicles. In the EU, where mobility systems are highly integrated, AI secures vehicle-to-everything (V2X) communications, connected infrastructure, and data networks from sophisticated cyber threats. With the rapid growth of passenger and freight traffic on cross-border routes in Moldova, Ukraine, and Romania, and the active implementation of smart mobility solutions, public administrations are faced with the need to ensure high cyber resilience of digital platforms. Large-scale AI projects require not only software but also a robust hardware infrastructure capable of securely processing and analyzing large amounts of geospatial and transportation data. In this context, the Fortinet Secure AI Data Center Blue Principle provides guidance for building secure data centers capable of supporting digital platforms like Connect2SmallPorts and EIT Urban Mobility RIS.

Key elements of such infrastructure include dedicated server clusters with high-performance CPUs and GPUs, enabling real-time data processing and training of artificial intelligence models to predict traffic flows, detect anomalies, and prevent cross-border criminal activity. Equally important are communications networks and routers with built-in cybersecurity, ensuring secure data exchange between transport hubs, border crossings, and mobility management centers. Storing large amounts of data requires scalable and fault-tolerant storage systems with encryption and backup support, ensuring the safety of both structured and unstructured data. Security and monitoring systems such as FortiGate, FortiNAC, and FortiAI are also essential, protecting the infrastructure from external threats, as well as providing access control, logging, and audit trails for all data transactions.

To complement the described infrastructure components, it is important to illustrate how cybersecurity-driven AI solutions are integrated into smart mobility environments. In particular, specialized platforms such as FortAI act as a central intelligence layer for monitoring, analyzing, and protecting transport and logistics data flows in real time. To further clarify the operational role of cybersecurity-driven AI within the proposed architecture, a dedicated conceptual visualization is provided. The following figure 3

presents the conceptual role of FortAI as a secured engine enabling cyber-resilient smart mobility operations across cross-border transport systems.



Fig. 3. FortAI: The secured engine of smart mobility
Source: created by the authors.

As shown in the figure, FortAI operates as an integrated cybersecurity and AI analytics layer that connects transport infrastructure, data platforms, and security monitoring systems into a unified operational environment. It enables continuous anomaly detection, predictive threat analysis, and automated response mechanisms for cross-border transport networks. By interfacing with SDI and ITS systems, FortAI ensures secure data exchange between border checkpoints, urban mobility hubs, and logistics corridors. This integration strengthens the resilience of smart mobility systems, supports compliance with EU cybersecurity requirements, and enhances the overall reliability and safety of transport operations in Moldova, Ukraine, and Romania.

These solutions enable administrations in eastern Moldova and border regions of Ukraine to integrate FortAI to monitor suspicious traffic patterns, coordinate law enforcement actions, and analyze large data streams using AI algorithms. Finally, AI management and orchestration tools enable centralized control of model deployment, manage computing resources, and ensure compatibility with national and cross-border SDI and ITS platforms. Together, these solutions create the conditions for secure, resilient, and efficient smart mobility in accordance with European cybersecurity and data protection standards. To effectively deploy large-scale AI projects in smart mobility and cross-border security, public administrations must consider both software and hardware infrastructure components. To further strengthen system robustness, it is essential to ensure continuous interoperability between AI-driven mobility platforms and national cybersecurity frameworks, enabling real-time information sharing and coordinated response across borders. In addition, the implementation of standardized data governance and secure API-based integration mechanisms supports scalable deployment of intelligent transport solutions while maintaining compliance with EU regulatory requirements.

As shown in Table 1, key elements include dedicated server clusters, secure networks, data storage systems, and AI monitoring and orchestration tools. These components provide high computing power for analyzing passenger and cargo flows, threat prediction, and anomaly detection, and protect critical transport infrastructure data and geospatial data stored in the SDI. This architecture enables the integration of solutions such as FortAI, Connect2SmallPorts, and EIT Urban Mobility RIS to ensure secure real-time monitoring, coordination between transport and law enforcement agencies, and compliance with European cybersecurity and data protection standards [13,14].

Table 1: Equipment Required for Secure AI Deployment

Infrastructure component	**Purpose**	**Connection with cybersecurity and smart mobility**
Server clusters with GPU/CPU	Big data processing, training AI models	Support for AI-based traffic flow monitoring and threat prediction
Communication networks and routers	Ensuring secure data transfer between nodes	Built-in IDS/IPS, network segmentation, protection against attacks on transport systems
Data storage systems (Storage)	Scalable and fault-tolerant storage of structured and unstructured data	Encryption and backup protect against data leaks and loss.
Security and monitoring systems (FortiGate, FortiNAC, FortiAI)	Cyber threat detection and prevention, access control	Ensure the resilience of AI platforms, anomaly monitoring, and SDI/ITS data protection
AI management and orchestration tools	Deployment, version control, resource management	Centralized model management, integration with SDI, ITS and cross-border platforms

Source: developed by authors

As shown in Table 1, the implementation of the listed components allows state administrations in the eastern part of the Republic of Moldova and the border regions of Ukraine to create a scalable and secure smart mobility infrastructure. Server clusters and data storage systems ensure the processing of large amounts of information and backup; secure networks and FortiGate/FortiAI monitoring systems prevent cyber threats; AI orchestration tools enable centralized management of computing resources and the integration of SDI and ITS data. This infrastructure organization guarantees secure data exchange between border crossings, transport hubs, and control centers, and supports the operation of the FortAI, Connect2SmallPorts, and EIT Urban Mobility RIS platforms, increasing resilience to cyber threats and compliance with European standards [13,14].

Implementing the components listed in Table 1 creates the necessary infrastructure for the secure operation of AI platforms in the fields of smart mobility and cross-border security. Based on this infrastructure, public administrations can integrate solutions like FortAI, enabling real-time incident prediction and prevention, optimizing traffic flows, and ensuring coordination between national and cross-border agencies. This technology is particularly important for the eastern regions of the Republic of Moldova and border crossings in Ukraine, where large international passenger and cargo flows occur. For example, at the Palanca-Reni and Ocnița-Soroca border crossings, FortAI can analyze vehicle and passenger traffic data, identify anomalies that may indicate smuggling or other cross-border criminal activity, and automatically notify the appropriate authorities.

Similarly, in small ports on the Dniester and Danube, FortAI's integration with Connect2SmallPorts platforms enables shipping monitoring, delay prediction, and optimization of logistics routes. In cities with high traffic density, such as Chisinau, Odesa, and Iasi, FortAI, in collaboration with EIT Urban Mobility RIS, enables dynamic passenger flow management, improves public transport operations, and enhances traffic safety through the early detection of potential threats. Thus, FortAI's integration, based on the infrastructure described in Table 1, creates the conditions for the digital transformation of smart mobility, enhances the cyber resilience of transport systems, ensures compliance with EU data protection standards, and facilitates effective coordination between countries in the region. This approach demonstrates how modern AI solutions can be applied in real-world cross-border interactions to improve the safety, efficiency, and resilience of the transport network.

4. European practices for sustainable and cyber-secure cross-border mobility: environmental and social components in Moldova and Ukraine

European experience in smart mobility demonstrates how digitalization, the integration of artificial intelligence, and standardized platforms can improve the efficiency, safety, and sustainability of transport systems. Platforms such as Connect2SmallPorts and EIT Urban Mobility RIS facilitate the monitoring of transport flows, data harmonization, and coordination between various authorities. They also promote environmental and social sustainability by minimizing CO_2 emissions, optimizing routes, and increasing accessibility to transport services for all population groups. These initiatives are supported by European Union missions and programs focused on cross-border cooperation, digital transformation, and compliance with cybersecurity standards.

The X4ITS (Cross for ITS) project is a shining example of coordinated cross-border and interregional cooperation in the field of intelligent transport systems in Central and Eastern Europe. It brings together government agencies, cities, public transport operators, the rail industry, road administrations, and transport information providers to implement coordinated and synchronized ITS applications on major roads and at the urban nodes connected to these routes. Building on the work of the previous phases of the CROCODILE project, X4ITS aims to:

- improving data collection, processing and access capabilities, including installing equipment, upgrading processes and integrating with National Access Points;
- ensuring the transmission of information on secondary roads and multimodal transport hubs, which is especially important for countries with intensive cross-border traffic and different languages;
- joint work on assessing the environmental and safety impacts, including the project's impact on decarbonization, digitalization of the transport sector, and accident reduction within the framework of the Vision Zero concept.

For Moldova and Ukraine, the X4ITS project is particularly relevant in border areas and small towns. Living labs are testing collaborative digital government services related to spatial planning, sustainable development, and smart small towns and villages. FortAI enables real-time detection of traffic anomalies, the prevention of cross-border crime, and

the cyber resilience of data integrated with the Connect2SmallPorts and EIT Urban Mobility RIS platforms.

The practical significance of these approaches is demonstrated by specific examples:

- Border crossings Palanca-Reni and Ocnița-Soroca: monitoring of transport and passenger flows, optimization of queues and warning of possible security threats;
- Small ports on the Dniester and Danube: improving shipping management, predicting delays and reducing environmental impact;
- Cities with high traffic density (Chisinau, Odessa, Iasi): optimising public transport routes, reducing waiting times and emissions, improving social accessibility and safety.

To provide a clearer understanding of how these European approaches are applied in practice, it is useful to present selected regional implementation cases. These examples illustrate how digital platforms, AI-based monitoring systems, and cross-border coordination mechanisms operate in real transport environments across Moldova, Ukraine, and Romania. The following figure 4, summarizes key diagnostic case studies of smart mobility implementation in border crossings, port infrastructure, and urban transport systems.



Fig. 4. Regional implementation: diagnostic case studies of smart mobility systems
Source: created by the authors

As illustrated in Figure 4, the selected case studies demonstrate the practical application of integrated smart mobility solutions in different spatial contexts. Border crossings such as Palanca–Reni and Ocnița–Soroca benefit from improved traffic monitoring, queue optimization, and enhanced security control. River and maritime hubs along the Dniester and Danube corridors achieve more efficient logistics management and reduced environmental impacts through predictive analytics. In urban centers including Chisinau, Odesa, and Iași, AI-driven transport optimization improves public transport performance, reduces congestion, and increases accessibility. Collectively, these implementations confirm the scalability of the proposed approach and highlight its relevance for strengthening cyber-resilient, sustainable, and interoperable cross-border mobility systems

in the region. Thus, the integration of European practices, modern digital platforms, and X4ITS solutions creates a comprehensive cross-border mobility ecosystem that simultaneously ensures:

- Cyber resilience and data security,
- Environmental sustainability and emission reduction,
- Social sustainability and improving the quality of transport services,
- Cross-border and interregional cooperation, promoting integration into

European transport and digital networks.

This approach demonstrates how European standards and technologies can be localised to address the real-world challenges of the border regions of Moldova and Ukraine, ensuring sustainable, safe and highly efficient development of smart mobility.

Sustainable mobility is a key component of cyber-resilient intelligent transportation systems. The integration of AI and digital platforms enables the optimization of transport routes and modes to minimize environmental impacts, particularly greenhouse gas emissions and local air pollution [27]. Real-time geospatial traffic data enables dynamic planning of freight and passenger transportation, reducing congestion and fuel consumption.

Environmental benefits include:

- Reducing CO_2 emissions through optimised logistics;
- Integrating electric vehicles and charging infrastructure using predictive analytics;
- Monitoring and reporting of environmental performance indicators in a transboundary context, allowing for joint assessment by Moldova, Ukraine and Romania .

Social sustainability - is no less important. Intelligent mobility systems improve accessibility, inclusiveness, and safety for all users, including vulnerable groups. Digital platforms enable the collection of user feedback and availability metrics, which AI systems use to optimize transport services in real time . For example, feedback on border waiting times can be immediately processed to adjust schedules or recommend alternative routes. Cross-border coordination enhances both environmental and social aspects. By sharing best practices and data through cross-regional platforms, transport authorities can jointly monitor sustainability indicators, align infrastructure investments, and implement common mobility policies in line with EU goals, such as the European Green Deal and the Sustainable and Smart Mobility Strategy [8,9].

The Connect2SmallPorts project exemplifies the digital transformation of small ports and the sustainability of smart cross-border mobility in the EU. It aims to implement digital technologies, including blockchain and IoT, in small ports in the Southern Baltic, where their application is limited and not integrated cross-border. Analysis revealed significant differences in port digitalization: Wismar, Karlskrona, and Klaipėda are actively developing their IT infrastructure, while Polish ports remain on a classic infrastructure path without a digitalization strategy. This creates a gap in the development of the intelligent

transport network and highlights the need for standardization and integration of solutions cross-border. The project aims to address the real challenges of "blue growth" by enhancing the IT and infrastructure potential of small ports, which is directly related to the development of cross-border mobility. Key measures include:

1. Digital audit of ports – assessment of the level of digitalization, optimization of logistics flows and increasing the efficiency of transportation;
2. Blockchain and IoT Strategy – transparency of transportation, data integration and reduction of environmental impact;
3. Pilot projects– five demonstration implementations of technologies in the region's ports, adapted to local infrastructure;
4. Creating sustainable value – integrating digital strategies into educational programmes and holding an annual Small Ports Digital Forum with awards for achievements in sustainable mobility.

The implementation of Connect2SmallPorts has cross-border implications. Digital platforms enable the harmonization of operations between countries, ensuring joint management of transport flows, data cyber-resilience, and integration with European ITS and MaaS systems. This is particularly relevant for the border regions of Moldova and Ukraine, where infrastructure is limited and coordination of transport and environmental flows is critical. The project can directly support the EU Green Dniester–Black Sea Corridor initiative by enabling the digitalization of ports along the transport corridor. Collecting and integrating cargo flow and environmental data enables route optimization, reduction of CO_2 emissions, and increased sustainability of transportation. Furthermore, transparent flow management contributes to increased efficiency in the transport chain and integration with European green corridors. Particular attention is paid to the sustainability of settlements along the lower Dniester and the Dniester Estuary, where small ports and river hubs are crucial for the region's economy and ecology. The use of digital platforms enables:

- control the load on transport hubs and infrastructure;
- optimize passenger and freight transportation, minimizing the impact on populated areas;
- reduce environmental risks associated with water and air pollution;
- create conditions for the sustainable development of small towns and villages along the estuary through the integration of data on transport, ecology and social indicators.

The Connect2SmallPorts project thus exemplifies how the implementation of digital platforms, blockchain technologies, and IoT can improve the efficiency, sustainability, and cybersecurity of cross-border mobility, supporting environmental and social priorities, and creating practical solutions for integrating small ports and settlements along the lower Dniester into European transport and digital networks. FortAI technologies, focused on using AI for big data analysis and crime prevention, complement these initiatives. In the border areas of Moldova and Ukraine, FortAI enables public administrations to enhance the cyber resilience of all types of smart mobility, including passenger and freight transport, as well as small and medium-sized transport hubs. FortAI systems provide anomaly detection, threat prediction, and automation of security procedures, strengthening cross-

border cooperation [28] and protecting critical infrastructure. To complement the technological and operational dimensions of cross-border smart mobility, it is essential to consider its broader environmental and social implications. Modern transport systems are increasingly evaluated not only in terms of efficiency and security, but also through Environmental, Social, and Governance (ESG) [29] criteria. In this context, digital platforms and AI-based solutions contribute to reducing emissions, improving accessibility, and strengthening social inclusiveness across transport networks. The following figure 5, illustrates the ESG dimension of smart mobility beyond traditional traffic management.



Fig. 5. Beyond traffic: Environmental, Social, Governance (ESG) dimensions of smart mobility
Source: created by the authors.

As shown in the figure, the ESG perspective extends the scope of smart mobility systems beyond operational efficiency to include environmental sustainability and social well-being. AI-driven optimization of transport routes contributes to significant reductions in CO_2 emissions and energy consumption, while digital monitoring systems support the integration of electric mobility and greener logistics solutions. From a social perspective, improved accessibility, real-time information systems, and user-centered transport services enhance inclusiveness and safety for diverse population groups, including vulnerable users. In addition, governance mechanisms based on data transparency, interoperability, and cybersecurity compliance ensure accountable and resilient transport management. Together, these dimensions reinforce the role of digital platforms such as Connect2SmallPorts and FortAI in promoting a sustainable, secure, and socially responsible cross-border mobility ecosystem. The combination of X4ITS, Connect2SmallPorts approaches and FortAI as a AI mobility start-up [30] demonstrates a synergistic effect for the sustainable development of regional mobility. The use of digital platforms and AI increases data transparency and reliability, integrates environmental and social indicators into transport management, and creates a sustainable foundation for small towns and villages to adapt to the modern requirements of a digital and green economy. Thus, European practices, adapted to the border conditions of Moldova and Ukraine as a associate countris to Three Seath Initiative [31], demonstrate that cyber-resilient digital mobility can become a tool for environmental, social, and economic sustainability,

strengthening international cooperation, reducing environmental impacts, and improving quality of life in communities in the lower Dniester and Dniester estuary regions.

5. Conclusions and strategic recommendations

This study demonstrates that the integration of artificial intelligence, digital platforms, and cybersecurity measures can significantly improve cross-border smart mobility in Moldova, Ukraine, and Romania. Key findings include:

1. Cyber-resilient infrastructure - coordination of national and transnational security command centers ensures secure handling of sensitive transport, geospatial and social data, while AI-based monitoring ensures predictive threat detection [32].
2. Operational efficiency - intelligent transport systems and digital audit platforms optimize passenger and freight flows, reducing waiting times and environmental impacts.
3. Regional cooperation and innovation - integration into interregional platforms such as Smart Cybersecurity Regions facilitates knowledge sharing, standardization of procedures and joint response to cyber incidents .

Strategic recommendations - for policymakers and transport authorities:

- Establish national border security operational management centres that comply with EU cybersecurity standards and ensure transnational coordination in managing the movement of people across borders;
- Expanding ITS and MaaS platforms for dynamic transport management using AI to forecast demand and optimize routes;
- Use valuable datasets (geospatial, transport, environmental, social) for real-time decision-making and sustainability monitoring;
- Strengthen participation in the Smart Regions for Cybersecurity programmes and related EU networks to exchange best practices, jointly develop solutions and train personnel in cross-border cybersecurity scenarios;
- Promote the implementation of shared environmental and social indicators to align cross-border transport policies with the objectives of the European Green Deal and the Sustainable and Smart Mobility Strategy.

The implementation of these recommendations will enable Moldova, Ukraine and Romania to improve the efficiency, sustainability and resilience of their transport systems, and lay the foundation for deeper integration into the EU digital and mobility ecosystem.

References

[1] C. Vrabie, "Artificial Intelligence Prospects for Public Organizations and Smart Cities", Digital Transformation. Lecture Notes on Business Information Processing, Vol. 465, 8-12, 2022. https://smart-edu-hub.eu/files/Proceedings/Smart_Cities_Orasul_Inteligent_Accelerating_innovation_2022.pdf

[2] V. Baltac, "Smart Cities - A Social Perspective", Smart Cities, Vol. 2, No. 4, 2019: https://www.mdpi.com/2624-6511/2/4/33 ;

[3] European Commission, "The Three Seas Initiative: Regional Cooperation and Connectivity", EC, Brussels, 2022. https://www.atlanticcouncil.org/programs/europe-center/the-three-seas-initiative/ ;

[4] ZAWIESKA Jakub; LODI Chiara, Joint Research Centre, “Research and innovation in Smart Mobility in Europe”: https://publications.jrc.ec.europa.eu/repository/handle/JRC143360 ;

[5] S. Serdyuk, Ilarion BOLGAR, Anatolii BABIN, Ion COVALENCO, "Aspects of cybersecurity specialist training for electric vehicle driver education in communities supporting cross-border electromobility": https://book-series.scrd.eu/index.php/bs/catalog/view/7/13/33 ;
[6] Joint Research Center EU Commission, «Digital Regional Data Space Infrastructures» (DRDSI), 2015: https://data.europa.eu/en/publications/use-cases/danube-reference-data-and-services-infrastructure-drdsi
[7] EU Commission, Intelligent Transport Systems are improving EU mobility, 2025: https://cinea.ec.europa.eu/programmes/connecting-europe-facility/transport-infrastructure/intelligent-transport-systems-eu_en ;
[8] EU Commission, Connect2SmallPorts, "Digital Audit Platform for Transport Hubs," 2021.: https://www.connect2smallports.eu ;
[9] EIT Urban Mobility, "RIS Digital Platforms for Intelligent Transport," 2021: https://www.eiturbanmobility.eu/ris_;
[10] Interreg Danube Region Programme, "X4ITS (Cross for ITS): Harmonised and synchronised Intelligent Transport Systems for cross-border mobility in the Danube Region", 2024. Available at: https://www.interreg-danube.eu/projects/x4its ;
[11] EU, "EU ITS Platform" (EU EIP): https://www.its-platform.eu/achievement/integrating-c-its-into-road-operators-day-to-day-business/#elf_l1_Lw ;
[12] EU Commission, TEN-T Maps of the Indicative Extension to Neighbouring Countries https://transport.ec.europa.eu/transport-themes/infrastructure-and-investment/trans-european-transport-network-ten-t/tentec-information-system-and-ten-t-map-library/ten-t-maps-indicative-extension-neighbouring-countries_en ;
[13] EU Commission, Data protection: https://commission.europa.eu/law/law-topic/data-protection_en ;
[14] EU, The JRC supports EU policy on cyber resilience by mapping cybersecurity standards: https://joint-research-centre.ec.europa.eu/projects-and-activities/cyber-security-standards_en ;
[15] EU Commission, DG TRANSPORT, «Status of the Pan- European transport corridors and transport areas: development and activities in 2000 and 2001: https://ec.europa.eu/ten/transport/external_dimension/hlg/2005_03_31_tent_consultation/doc/corridor_status_report_2000_2001_en.pdf;
[16] EU Commsiion, CROCODILE (Cooperation of Road Operators for Crocodile) corridor: https://www.its-platform.eu/its-corridors/crocodile/ ;
[17] EU Commission, European Space Agency, « ESA inaugurates new Cyber Security Operations Centre», 2025 : https://www.esa.int/Space_Safety/Cyber_resilience/ESA_inaugurates_new_Cyber_Security_Operations_Centre ;
[18] EU Commission, Communisty of Practices S3 "Smart Regions for Cybersecurity", 2023.: https://ec.europa.eu/regional_policy/policy/communities-and-networks/s3-community-of-practice/partnership_industrial_mod_cybersecurity_smart_regions_en ;
[19] JRC EU Commission, «Artificial intelligence and data», 2026: https://joint-research-centre.ec.europa.eu/scientific-portfolios/ai-and-data_en ;
[20] EU, REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL : https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng ;
[21] EU Commission, "Monitoring the uptake and impact of AI applications in the Mobility and Transport sectors", 2025: https://ai-watch.ec.europa.eu/topics/transport-and-mobility_en ;
[22] EU Commission, "Creating a common European mobility data space", 2025: https://transport.ec.europa.eu/transport-themes/smart-mobility/creating-common-european-mobility-data-space_en ;
[23] European Commission, "Sustainable and Smart Mobility Strategy", Brussels, 2020.: https://transport.ec.europa.eu/smart-mobility_en ;
[24] EU Commission, "Deploying European 5G cross-border corridors", 2025: https://digital-strategy.ec.europa.eu/en/policies/cross-border-corridors ;
[25] EU Fortai - EU AI Act Compliance, https://www.fortai.eu/ ;
[26] AI adoption in the EU's Public Sector: an opportunity to better serve citizens and support startups: https://digital-strategy.ec.europa.eu/en/library/ai-adoption-eus-public-sector-opportunity-better-serve-citizens-and-support-startups ;

[27] UNECE, Long-term monitoring under the Air Convention delivers valuable insights into environmental impacts of air pollution, 2026: https://unece.org/biodiversity/press/long-term-monitoring-under-air-convention-delivers-valuable-insights ;
[28] NATO Cooperative Cyber Defence Centre of Excellence, "Cross-Border Cyber Incident Response", Tallinn, 2022. : https://ccdcoe.org ;
[29] EU, Environmental, social and governance (ESG) ratings: Council greenlights new regulation https://www.consilium.europa.eu/en/press/press-releases/2024/11/19/environmental-social-and-governance-esg-ratings-council-greenlights-new-regulation/ ;
[30] Joint Research Centre, "Data-driven and AI-enabled Smart Mobility in European Cities," Joint Research Centre Reports, 2023: https://joint-research-centre.ec.europa.eu ;
[31] European Commission, "The Three Seas Initiative: Regional Cooperation and Connectivity", EC, Brussels, 2022: https://3seas.eu ;
[32] EU Commission, The Directive on the Resilience of Critical Entities entered into force on 16 January 2023 https://eur-lex.europa.eu/eli/dir/2022/2557/oj ;