Smart borders and digital corridors for ensuring security in NATO-oriented border areas: the Romania–Moldova–Ukraine case

Catalin VRABIE,
National University of Political Studies and public administration, Romania
catalin.vrabie@snspa.ro

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

Anatoly BABIN,
Academy of Economic Research of Moldova,
Chisinau, Republic of Moldova
anatolii.babin@ase.md

Hilarion BULGAR,
Researcher at the Institute of Perspective University INT,
Chisinau, Republic of Moldova
ilarionbolgar@gmail.com

Abstract

Objectives of the study: This paper examines how smart border concepts and digital corridor architectures can enhance border security, regional resilience, and sustainable mobility in the Romania–Moldova–Ukraine border region. It aims to demonstrate how geospatial and data interoperability standards aligned with NATO norms and the EU INSPIRE directive enable harmonized spatial data management supporting both defense and civilian applications. Prior Research: The paper builds on recent European initiatives in smart border management and geospatial data integration, including the EU Smart Borders package, INSPIRE implementation experiences, and NATO geospatial standards (NGMS, DIGEST). The study builds on previous work on geospatial interoperability and the application of digital twins in cross-border management. Methodology: A comparative case study method was used, combining spatial data analysis, policy review, and system architecture assessment. The study is based on publicly available datasets, defense geospatial frameworks, and documentation from pilot projects in the Danube region and the Eastern Partnership. Findings: The findings demonstrate that harmonized GIS infrastructures and cyber-resilient data exchange platforms can significantly improve situational awareness, operational coordination, and logistical efficiency. Digital corridors connecting border control nodes and regional transport infrastructure facilitate dual-use (military-civilian) mobility, enhance emergency response, and enable integrated monitoring of flows between jurisdictions. The analysis also places the Romania–Moldova–Ukraine corridor in the context of the broader Three Seas Initiative, highlighting its role in connecting the transport, energy, and digital networks of Central and Eastern Europe, as well as in enhancing the interoperability of NATO and EU infrastructures. Conclusions and Significance: The study offers practical recommendations for policymakers, defense planners, and regional authorities seeking to implement interoperable and secure border management systems compliant with NATO and EU standards. Scientific Value: The paper presents a strategic model for smart border management that integrates defense preparedness and sustainable development. It demonstrates how geospatial harmonization and digital interoperability can transform border regions into resilient, data-driven security and mobility ecosystems.

Keywords: geospatial interoperability, cyber resilience, dual-use infrastructure, border intelligence, regional resilience.

1. Introduction

The current transformation of the European and Euro-Atlantic security system is accompanied by profound structural changes in the organization of spatial, logistical, and information interactions between NATO member states, the European Union, and partner countries. Against the backdrop of geopolitical instability and the growth of hybrid threats, a new strategic planning framework is emerging, in which the digitalization of defense processes, cyber resilience, and the integration of dual-use infrastructure play a key role. In this context, the regions of Eastern Europe, primarily the Romania - Moldova - Ukraine axis, are becoming a space for the practical implementation of the concepts of Military Mobility 2.0 [1], Smart Borders [2], Host-Nation Support (HNS) [3], and Digital Transport Corridors [4]. Their development is aimed at ensuring infrastructure compatibility, harmonizing spatial data, and creating a single digital security space that combines defense and civilian functions.

The relevance of the study is determined by the need for a systematic analysis of the mechanisms for interfacing NATO standards (STANAG [5], AJP [6]) with EU directives (INSPIRE [7], TEN-T [8], EUROSUR [9]) and the digital logistics architecture (AEOLIX [10], FENIX [11]). Such integration allows not only to strengthen the defense capability of the region, but also to form a new model of sustainable development, where military mobility becomes an element of overall infrastructural and economic sustainability. The aim of this study is to develop a conceptual framework for the integration of Host-Nation Support, Military Mobility 2.0 and Smart Borders mechanisms in the Romania – Moldova - Ukraine border region, with an emphasis on geospatial data standardization, digital interoperability and the development of innovative ecosystems. The objectives of the study include:

- Analysis of the regulatory and institutional framework for Military Mobility 2.0 and Host-Nation Support;
- Definition of the architecture of digital and geographic information systems that ensure interdepartmental compatibility;
- Assessment of the potential for integrating EU initiatives (AEOLIX, Horizon Europe, Digital Europe Programme) into the HNS and Smart Borders structure;
- Development of practical recommendations for the implementation of digital governance tools in the context of regional defense capability.

The methodological framework incorporates principles of system analysis, geoinformation modeling, and comparative institutional analysis. The source material consists of NATO regulations (AJP-3.17, AJP-4.3, AJP-6, STANAG 7074, 2592), EU directives (INSPIRE, 2007/2/EC; Regulation 2017/2226/EU), as well as analytical reports from Frontex, JRC, EDA, and the European Commission. Thus, the article aims to identify points of intersection between NATO and EU defense, infrastructure, and digital strategies that could strengthen the resilience of Europe's eastern flank and improve the effectiveness of interactions between allies and partners.

2. Host-nation support and military mobility 2.0

The Host-Nation Support (HNS) concept is central to NATO's military mobility and strategic resilience. It defines the legal, logistical, and organizational mechanisms that ensure host nation support for allied forces during operations, exercises, and deployments. According to the Allied Joint Doctrine for Host-Nation Support (AJP-4.3) [3], HNS aims to provide allies with access to the infrastructure, services, and resources necessary to accomplish missions, as well as to create conditions for the compatibility of national and allied command and control systems. In the current context of the Military Mobility 2.0 initiative, the Host-Nation Support (HNS) doctrine is acquiring not only a logistical but also a strategic dimension related to the digitalization of movement planning and coordination processes.

The effectiveness of HNS is determined by the ability of national and allied structures to exchange information on transport corridors, resources, and infrastructure in real time. This is achieved through the use of interoperable digital platforms such as NATO Logistics Functional Area Services (LOGFAS), Movement Coordination Centre Europe (MCCe), and ESRI ArcGIS Enterprise, which enable the synchronization of data on routes, temporary hubs, border crossings, and dual-use assets. The integration of these tools into national movement management systems ensures transparency of logistics chains and reduces response times during cross-border operations. Furthermore, the use of geospatial analytics and STANAG 7074 (DIGEST) standards facilitates the creation of a unified situational picture for all participants - from NATO headquarters to regional coordination centers. The diagram below illustrates the architecture of interaction between host nations, allied forces, and international coordination structures within the framework of implementing HNS principles and troop movement planning.

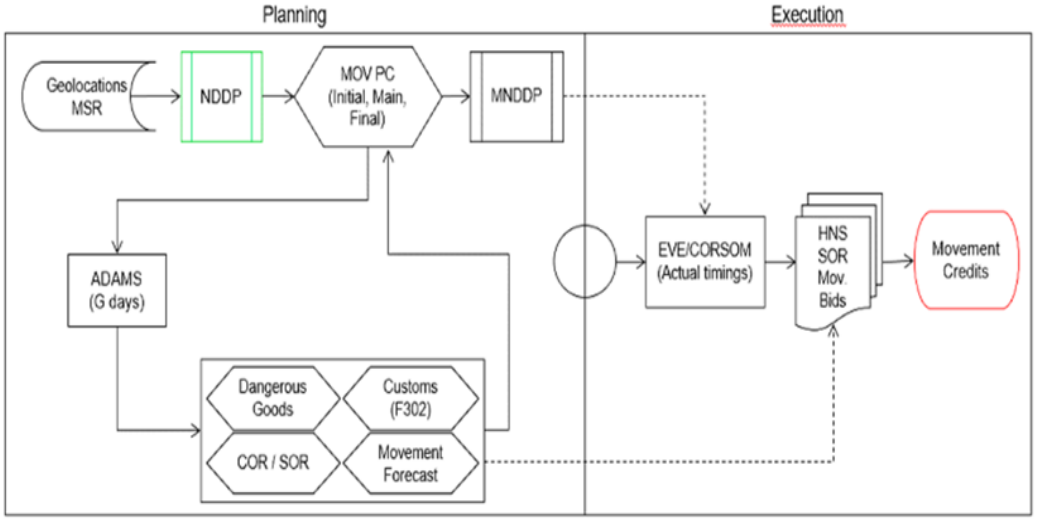

Fig. 1. Structure of HNS interaction and planning of troop and resource movements.
Source: Allied Joint Doctrine for Host-Nation Support (AJP-4.3) [3],

The figure depicts the architecture of interaction between the Host Nation, Allied Forces, Movement Coordination Centres Europe (MCCe), national logistics agencies, and Smart Border C2 components. Data flows and logistics chains are shown by arrows, from the strategic level - NATO JSEC and EDA - to the tactical level - regional HNS hubs and Smart Border Nodes. The diagram illustrates how digital tools (e.g., ArcGIS Enterprise and EUROSUR) integrate with military and humanitarian movement processes through cross-border corridors.

2.1. Spatial data harmonization and logistic compatibility

The Trans-European Transport Network is adapted for dual use. The TEN-T Regulation contains several elements to support military mobility within and outside the EU. Article 48 (Military Mobility) stipulates that when constructing or upgrading infrastructure on sections of the Trans-European Transport Network that intersect with the military transport network (as defined in the "Military Requirements for Military Mobility within and outside the EU", adopted by the Council on 26 June 20231), Member States shall take into account the need, relevance, and feasibility of exceeding the standard requirements set out in the TEN-T Regulation. Article 48 of the Military Mobility Regulation entrusts the Commission with the task of identifying priority corridors for military transport. Furthermore, the revised TEN-T Regulation improves and harmonizes various transport infrastructure standards with military requirements, particularly with regard to railways. In addition, updated TEN-T maps now more clearly reflect military needs, including the expansion of the network to neighboring countries such as Moldova and Ukraine.

The effective functioning of the HNS is impossible without the standardization of spatial data used in route planning, troop deployment, and supply coordination. The application of STANAG 7074 (DIGEST) [12], STANAG 2586, and STANAG 2592 standards ensures the compatibility of cartographic and geoinformation products, which is particularly important when national systems interact with NATO allies. Data harmonization involves the unification of formats, encodings, and metadata, as well as the use of common information exchange protocols. This creates the basis for the formation of a single information space, where data on routes, time nodes, infrastructure, and weather conditions is available in real time to all participants in the operation - from headquarters to field units. An example of the practical implementation of this approach is the Military Mobility 2.0 initiative, presented by the European Commission and the European External Action Service in 2025. Its main goal is to accelerate the cross-border movement of troops and equipment in Europe by harmonizing procedures, reducing administrative barriers, and digitalizing planning and monitoring processes. The Military Mobility 2.0 Action Plan includes:

- coordination of routes and infrastructure standards between EU countries and NATO partners;
- simplification of procedures for diplomatic permits and customs clearance;
- implementation of integrated digital platforms for the exchange of geospatial and logistics information;
- development of dual-use transport corridors (military and civilian).

- Military Mobility 2.0 is thus becoming a key tool for synchronising Europe's military and civilian infrastructure systems, facilitating not only operational mobility but also the continent's strategic resilience.

2.2 Regional dimension: Romania, Moldova and Ukraine

The application of HNS and Military Mobility 2.0 principles in the Romania-Moldova-Ukraine region is of particular importance. Romania, as a NATO and EU member, serves as the main logistics hub on the eastern flank, connecting the Black Sea region with Central Europe. Moldova, despite its neutral status, can serve as a host nation in dual-use civil-defense scenarios, providing infrastructure and data exchange channels within EU programs. Ukraine, a key NATO partner, is integrating HNS and Military Mobility elements into the restoration and modernization of its transport and military infrastructure, increasing its resilience and interoperability with allied systems. The implementation of digital solutions based on the AEOLIX and FENIX platforms allows for the unification of government and military information systems into a unified logistics architecture. These platforms support NATO Allied Command Transformation standards and enable automated data exchange between logistics centers and transport operators.

2.3. NATO and EU standards correspondence table in the HNS context

Table 1. Application of NATO and EU standards in the Host-Nation Support architecture

System component	Associated NATO/EU standard	Functional purpose	Application in the region
Geospatial data	STANAG 7074 (DIGEST), 2586, 2592	Compatibility and metadata exchange	Coordination of cartographic information between headquarters and national agencies
Communication networks	AJP-6, STANAG 5524, 4621	Cyber resilience and secure exchange	Secure data transfer between checkpoints and logistics centers
Logistics data	AEOLIX, FENIX	Supply chain transparency and analytics	Monitoring traffic flows along the Romania–Moldova–Ukraine axis
Operational coordination	AJP-3.17, AJP-4.4	Joint planning and mobility	Integration of transport and defense operations
Cybersecurity	AJP-3.20, STANAG 4774/4778	Data and communications protection	Responding to cyber incidents in edge networks

Source: Author's development

2.4. Practical impact and integration with digital platforms

The integration of HNS and Military Mobility 2.0 paves the way for the development of a unified situational awareness architecture - the Common Operational Picture (COP), which integrates data from military, civilian, and commercial sources. At the border region level, this ensures:

- reduction of time for coordination of operations;
- increasing the predictability of supply chains;
- integration of analytics, satellite surveillance and geographic information systems.

This approach not only enhances the region's defense capability, but also promotes economic development through more efficient use of dual-use infrastructure.

3. Smart borders and innovative ecosystems

The development of the Smart Borders concept in the European Union arose from the need to combine security, migration management, and economic efficiency into a single digital border management system. The program relies on technological, legal, and organizational tools to form the so-called Next Generation Border. Its key goals are to increase the transparency of movement, reduce administrative procedures, and ensure sustainable protection of the EU's external perimeter, including its eastern flank. The conceptual foundation of Smart Borders is formed by the Entry/Exit System (EES) and European Travel Information and Authorization System (ETIAS) [13], which integrate with the EUROSUR (European Border Surveillance System) platform. The latter collects and processes data from national border systems, satellite and unmanned surveillance systems, and maritime sensors, creating a multi-layered situational awareness picture.

3.1. Smart border architecture and integration levels

Before describing the Smart Borders architecture layers, it is important to note that the development of this system is taking place amidst the active convergence of defense and civilian digital governance tools. The European Commission and the Council of the EU view "Smart borders" not only as an element of movement control, but also as the foundation of a unified information and analytical infrastructure capable of responding to hybrid threats, cyber risks, and migration crises. Since 2023, the Interoperability Framework for Border and Security Data Systems initiative [14] has been integrating key databases (EES, ETIAS, VIS, SIS, Eurodac) into a common digital governance platform supported by the eu-LISA agency. This creates a unified data exchange framework in which civilian, border, and defense services operate according to standardized protocols. A key focus of this transformation is the development of end-to-end data interoperability standards that will enable the integration of national surveillance and control systems with NATO infrastructure. The use of STANAG 7074 (DIGEST), STANAG 5525 (Joint Operations Graphics), and the INSPIRE directive enables the spatial integration of data from diverse sources: the Galileo and Copernicus satellite systems, unmanned surveillance systems, Frontex geoportals, and national analytical centers. At the same time, the role of cyber resilience and data protection is strengthened: the implementation of Security by Design and Data Sovereignty principles is becoming mandatory for the deployment of national Smart Border components.

Regional initiatives such as the Three Seas Initiative and Military Mobility 2.0 play a significant role in this process, enabling the practical connection of infrastructure corridors,

transport networks, and communications channels with surveillance systems. Digital Security Bridges are being established along the Romania-Moldova-Ukraine axis, where data on vehicle movements, migration flows, and logistics operations are aggregated into cross-border situational awareness centers. These centers, deployed with the support of Frontex and NATO, provide not only operational surveillance but also the modeling of response scenarios, increasing the region's strategic resilience and strengthening its role as a link between NATO and EU structures. The modern Smart Borders architecture relies on the interaction of five functional layers:

1. Sensor Layer - integrates satellite surveillance, radar stations, video monitoring and unmanned platforms.
2. Communication Layer - ensures secure data transmission using NATO and EU protocols, including the use of encrypted Galileo PRS networks.
3. Data Analytics Layer – generates situational awareness based on the integration of data from Copernicus, Frontex, national agencies and private operators.
4. Decision Layer - includes algorithms for risk assessment, flow forecasting and access control automation.
5. Operational Layer - coordinates interaction between national and allied structures, including border services, Frontex and NATO communications security centres.

The EUROSUR framework, launched by the European Commission in 2013 [15] and the updated regulation of 2021 [16], are a logical development of this architecture. It already integrates AI and machine learning capabilities to analyze data streams in real time, enabling a shift from reactive to proactive risk management.

3.2. The role of regional digital corridors

On the EU's eastern flank, digital corridors are being developed as elements of the overall Military Mobility 2.0 framework, linking transport, energy, and communications hubs. The Romania–Moldova–Ukraine region plays a key role in this process, as it combines elements of civilian infrastructure with defense significance. Along the trans-European TEN-T routes, points of contact between military and civilian monitoring systems are being created, integrating data on transport flows and cargo movements into situational awareness centers. The operation of such corridors is impossible without the application of the INSPIRE Directive (2007/2/EC) geoinformation standards, which ensure the compatibility of spatial data. In practice, this is expressed in the formation of a unified repository of geospatial layers, including data on transport facilities, infrastructure, and administrative borders, accessible to both national and supranational users. To coordinate these processes, tools from the European Frontex agency, based on ESRI technologies (ArcGIS Enterprise, ArcGIS Hub, StoryMaps), are actively used [17]. These solutions provide dynamic situational map updates and the integration of video feeds, sensor data, and satellite imagery. Furthermore, ESRI platforms enable real-time spatial analysis, identifying high-risk areas and optimizing patrol routes.

3.3 Application in partner countries

Moldova, Romania, and Ukraine are gradually adapting these tools to their national needs. In Romania, the implementation of the ArcGIS Hub platform has enabled the creation of a

National Border Management Situation Center, integrated with Frontex and EU systems. In Moldova, with the support of the EUBAM mission, ArcGIS Pro tools are being implemented to monitor border activity and share data with neighboring countries. In Ukraine, ESRI solutions are being used in the digitalization of border services, enabling integration with the Copernicus surveillance systems and the national Delta and Harpoon platforms. These measures aim to gradually integrate Eastern European countries into the European digital border architecture, where threat and movement data become part of a unified EU and NATO situational awareness system.

3.4. Smart Border Integration Levels Table

Table 2. Multi-layered architecture of Smart Borders in Eastern Europe

Level	Technological tool	European program	Regional application
Sensor Layer	Copernicus, Galileo PRS	EU Space Programme	Satellite monitoring and time synchronization of operations
Communication Layer	Galileo PRS, STANAG 4621	NATO–EU Interoperability	Secure data transfer between border posts
Data Analytics Layer	AI/ML modules, Frontex Risk Engine	EUROSUR Step 4	Flow analysis and threat forecasting
Decision Layer	Frontex Interoperability Hub	EES–ETIAS	Automation of edge solutions
Operational Layer	ArcGIS Enterprise, INSPIRE	Digital Europe Programme	National and cross-border situational maps

Source: Author's development

3.5. Impact on the stability and security of the region

The implementation of Smart Borders and digital corridors creates the preconditions for the transition from fragmented surveillance systems to a unified space for defense and civilian coordination. This is particularly important for the eastern flank, where hybrid threats combine with migration, energy, and cyber risks. Ensuring synergy between NATO and EU systems is becoming a factor in the region's strategic resilience, and the use of ESRI and Frontex digital tools makes these processes manageable and replicable at the interstate level.

4. Innovative ecosystems and intellectual property

The development of a digital security architecture requires an innovation foundation capable of supporting a continuous flow of research, development, and implementation. The Horizon Europe, Digital Europe, and European Defence Fund (EDF) programs are creating a structural foundation for the formation of so-called Security Innovation Ecosystems. These ecosystems unite research centers, universities, startups, and defense companies into common consortia, where collaboration is based on the principles of open innovation and intellectual property protection. Intellectual Property Rights (IPR) is becoming a key element of this model-not only as a legal instrument but also as a means of protecting the EU's technological sovereignty.

4.1. Integration of NATO standards, innovative solutions and foreign economic activity in the smart border ecosystem

The integration of Horizon Europe's innovative solutions, R&D results, and EUROSUR with intellectual property protection mechanisms creates the foundation for a smart and secure economic ecosystem, where digital technologies ensure not only effective control over the movement of goods and data but also the protection of intellectual property. Thus, the development of a "Smart border" is becoming not just a security tool but also a strategic mechanism for supporting international trade, innovation exchange, and the digital sovereignty of the EU and partner countries. When examining the protection of intellectual property rights (IPR), the role of the "smart border" and regional administrations in the development of the market for scientific and technological information and intellectual capital arises. The "Smart border" concept, integrating digital technologies, R&D, and cybersecurity mechanisms, can serve as a platform not only for controlling the movement of goods and data but also for encompassing the activities of institutional innovation organizations operating within the framework of the Science and Innovation Code of the Republic of Moldova (Article 87, 2020). In particular, scientific and technological information, sold as information products, has the status of a commodity and forms a market for scientific and technological information products, accessible to all individuals and legal entities, regardless of ownership. In this context, the "smart border" can ensure:

- Digital integration of scientific and technological products into cross-border exchange chains with partners from the EU and NATO countries, including the export and import of information products, intellectual property, and innovative services.
- Monitoring and verifying intellectual property rights at the regional and international levels, which is critical for protecting innovation and ensuring compliance with contractual obligations in foreign economic activity.
- Supporting institutional innovation organizations in gaining access to intellectual capital markets by stimulating knowledge exchange, commercialization of R&D, and technology transfer.

4.2. The role of universities and the private sector

University laboratories and private companies participating in the Horizon Europe and Digital Europe Programmes are becoming a key element of the innovation ecosystem. They provide an influx of ideas and talent capable of developing new technological solutions in AI, cybersecurity, and situational analysis systems.

The development of a "Smart border" ecosystem is impossible without sustainable collaboration between the academic, private, and public sectors, which forms the foundation of the region's innovative potential. University research centers and laboratories act as drivers of technology transfer and the generation of new solutions in data analysis, cyber resilience, and digital logistics. The private sector, including software developers, telecom operators, and IT solution integrators, ensures the practical implementation of these innovations in border management infrastructure. In Eastern European countries, universities are joining the Horizon Europe and Digital Europe Programme application consortia, where joint projects are being developed with defense and transport ministries. This model facilitates the implementation of NATO standards (STANAG, AJP) in civilian

applications, enhancing the dual-use potential of technologies and reducing the fragmentation of digital solutions. The structural diagram below reflects the relationship between NATO standards, academic and industrial structures, and foreign economic activity mechanisms in the Smart Border ecosystem. The smooth transition from the role of universities and the private sector to the framework is realized through the recognition that academic and industrial-technological initiatives do not exist in a vacuum. Their efforts are integrated into a unified system of standards and processes that ensures compatibility with NATO and EU requirements. The following framework illustrates the relationship between research centers, businesses, and foreign economic activity mechanisms in the context of the "smart border" ecosystem.

4.3. Structural diagram of the "Integration of NATO standards, innovation and foreign economic activity in the smart border ecosystem"

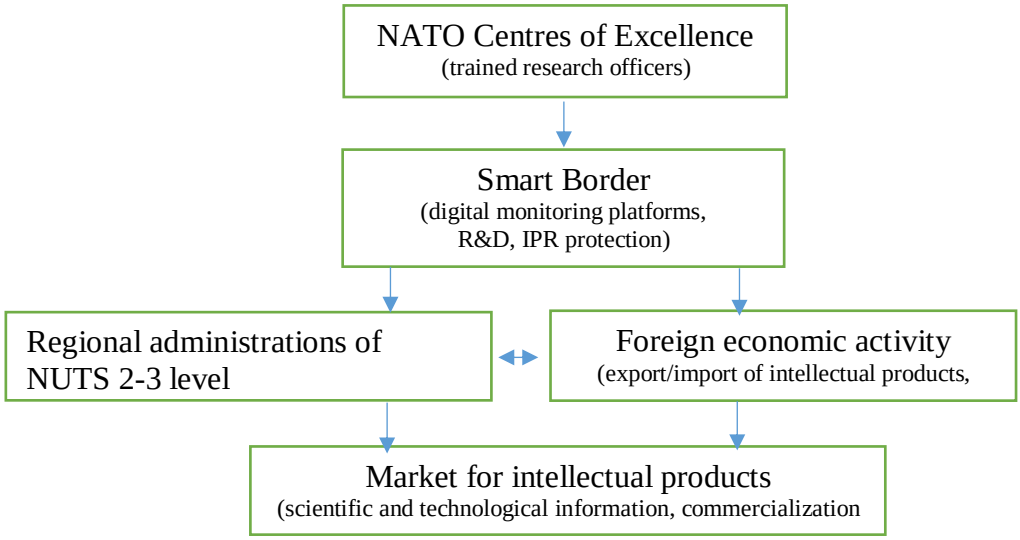

Fig. 2. Structural diagram of the interaction of key elements of the "smart border" concept and NATO standards in the cross-border space of Romania, Moldova and Ukraine
Source: compiled by the author

As the diagram illustrates, the collaboration between universities, private companies, and government agencies creates a closed innovation loop, where scientific results are transformed into applied technologies for surveillance systems, analytics, and logistics management. University laboratories provide the methodological and research foundation - from prototyping artificial intelligence algorithms to developing situational awareness interfaces. The private sector is responsible for adapting and scaling these solutions into national and regional information systems, ensuring their compatibility with EU and NATO infrastructure. Foreign economic activity (FEA) becomes a mechanism for implementing innovation through technology exchange, licensing, and cross-border investment. This creates an integrated environment where NATO standards and civilian

innovations do not compete but rather mutually reinforce each other, forming a sustainable digital architecture for security and development in the Romania–Moldova–Ukraine region.

4.4. Implications for regional sustainability

The formation of innovative ecosystems based on the secure exchange of intellectual property creates long-term potential for sustainability and technological independence. The Eastern flank of Europe has the opportunity not only to adapt existing EU solutions, but also to contribute to the development of common digital standards, ensuring a balance between security, innovation, and economic development. An additional factor in strengthening regional resilience is the systemic integration of digital and defense infrastructures, which makes it possible to create a single space for the exchange of information between the regions of the Eastern flank states and the EU. One of the key elements of Phase I and Phase II of the EUROSUR roadmap (Table 4) is Step 4 - "Exploitation of R&D (FP7) [18] to improve and test the performance of surveillance tools" - and this is where the role of universities and research-research centers is becoming strategic.

Universities and laboratories not only act as providers of innovation and technological solutions -sensor systems, geospatial data processing algorithms, and virtual border models - but also as platforms for field testing, impact assessment, and verification of new tools. In the Romania-Moldova-Ukraine region, the inclusion of academic institutions in national "smart border" plans enables the implementation of Step 4 through the creation of joint consortia, connection to European R&D programs, and testing of infrastructure on real border sites. Such participation facilitates not only technological transformation but also the development of human resources, making university-Industrial cooperation is a cornerstone of sustainable implementation of border security architecture.

Phases	Steps
Phase I Interlinking and streamlining existing surveillance systems at national level	**Step 1:** Setting up of *national coordination centres (NCCs)* for border surveillance in the Member States located at the eastern and southern Schengen external borders.
	Step 2: Setting up of the *EUROSUR network*.
	Step 3: Cooperation with *neighbouring third countries* to enhance their capacity to manage their own borders, fight cross-border crime and fulfil their search and rescue responsibilities.
Phase II Development of common tools for border surveillance at EU level	**Step 4:** Exploitation of *R&D (FP7)* to improve and test the performance of surveillance tools, e.g. to detect small boats.
	Step 5: Setting up of a service for the *common application of surveillance tools* (satellites, ship reporting systems, etc.).
	Step 6: Setting up of the *Common Pre-frontier Intelligence Picture*
Phase III Creation of a common information sharing environment for the EU maritime domain	**Step 7:** Creation of a *common information sharing environment* for internal security purposes covering the southern maritime borders.
	Step 8: Creation of a *common information sharing environment* for the EU maritime domain, covering all maritime activities (border control, law enforcement, customs, maritime safety, marine environment, fisheries control, defence).

Fig. 3. Steps and phases identified in the 2008 EUROSUR roadmap
Source: EUROSUR roadmap 2008 [18]

This table presents the original EUROSUR roadmap-2008, which included three phases and eight steps to develop a system of video surveillance and data exchange at the EU's external borders. Although the document is aimed at countries-members and was aimed at launching before 2013, its logic remains useful - in particular for countries-candidates (Moldova, Ukraine) as a model for transition: from the creation of national coordination centers and data collection to the construction of a common information environment.

Adapted for the Romanian region-Moldova-Ukraine needs to consider its specific land and river borders, institutional structure, and the need for interoperability with the Smart Borders architecture.

4.5 Smart technologies and artificial intelligence in the smart border system

Contemporary challenges in security, migration, and cyber resilience require the systemic integration of artificial intelligence (AI) technologies into external border management processes. The Smart Border architecture utilizes AI [19] as a key tool:

- to automate the collection and analysis of real-time data from ground, air and cyber sources;
- to predict threats and identify abnormal behavior patterns based on machine learning algorithms;
- to optimize transport and logistics flows, including monitoring the capacity of supply points and routes;
- to support situational response and strategic decision-making in crisis situations or cross-border operations.

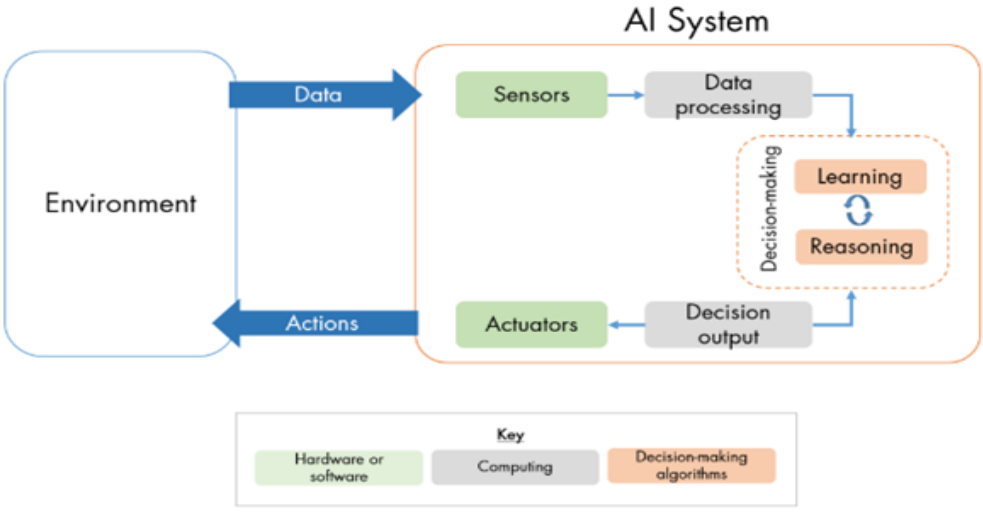

Fig. 4. Components of an AI system
Source: RAND Europe adapted from European Commission [19]

AI integrates with NATO geoinformation standards (NGMS, DIGEST, STANAG 7074) and EU systems (EES, ETIAS, EUROSUR), creating a cyber-resilient data architecture

that enables the unification of innovation, intellectual property management, and cross-border foreign economic activity. The algorithms used provide intelligent information filtering and the identification of hidden relationships between data coming from sensor systems, satellites, unmanned platforms, and logistics networks. At the situational management level, AI is integrated into the Common Operational Picture (COP), which complies with STANAG 5525, creating a unified visual and analytical environment for civil and military services. Key functional elements of AI systems within Smart Border:

- Sensor layer (Data Acquisition Layer) - collection of data from physical and digital sources, including military and civilian sensor networks (STANAG 4559).
- Data Processing Layer – filtering, normalization and preliminary analysis of information, ensuring data reliability.
- Algorithmic level (Decision Layer) - application of machine learning and neural networks to predict threats and optimize logistics flows (AJP-5).
- Action & Response Layer – implementation of decisions through route adjustments, protocol activation and integration with MCCe systems.

The use of AI makes it possible to create a unified, cyber-resilient control loop that integrates data from different agencies and countries, reducing administrative costs and speeding up the flow of transport and humanitarian aid.

4.6. Roadmap for ensuring defense capability by 2030

Modern European security requires not only effective border management and smart technologies, but also strategic long-term defense capability planning. The Roadmap for European Defense Capabilities by 2030 [20] is a comprehensive plan that integrates national and regional efforts with the priorities of the European Union and NATO, setting clear goals, timeframes, and performance indicators. The roadmap's primary objective is to ensure the coordinated development of armed forces, infrastructure, technologies, and digital platforms capable of countering modern threats, including hybrid and cyber threats. The document includes four key areas proposed by the European Commission to the European Council:

- The European Counter-UAS Initiative (Counter-UAS) – development of national and joint drone detection and neutralization systems, integration with Smart Border early warning systems.
- Eastern Flank Surveillance - strengthening satellite, air and ground monitoring to promptly identify threats on strategically vulnerable borders.
- European Air Shield - the formation of a unified air defense with the integration of data from national air defense systems, drones and AI modules for threat prediction.
- European Space Shield - protection of space infrastructure, satellite communication links and GPS/Galileo systems, which are critical for navigation and situational management at borders.

These initiatives strengthen Europe's ability to defend itself on land, in the air, at sea, in cyberspace and in space, while directly contributing to NATO's goals of enhancing joint defence capability and the resilience of strategic lines of communication.

The relationship with Smart Border and AI systems within the 2030 Roadmap is that it is logically linked to the Smart Border architecture and AI systems.

5. Practical significance for regional security

The implementation of the Roadmap ensures increased strategic autonomy, reduced dependence on individual technology suppliers, and stronger integration of national systems into the EU and NATO frameworks. In the context of Europe's eastern flank, this means:

- Ability to quickly respond to crisis situations, including migration flows and hybrid threats;
- Formation of a regional digital security ecosystem where data, analytics and decisions are made jointly;
- Strengthening cooperation with the EU and NATO, creating platforms for knowledge sharing and joint technology development;
- Supporting national innovation ecosystems through intellectual property exchange, joint R&D projects, and pilot technological implementations.

The Roadmap to 2030 thus serves as a bridge between strategic planning and the operational implementation of Smart Border technologies, enabling joint efforts at national, regional and European levels.

5.1 Using digital twins for more efficient border management in Romania, Moldova and Ukraine

The Eastern European Border Twin Model [21], based on Frontex's experience, provides a realistic and flexible platform for testing and simulating situations at the external borders of the EU and neighboring territories. It enables border guards and law enforcement officials in Romania, Moldova, and Ukraine to simulate specific scenarios-from natural disasters that hinder border crossings to attempts at human trafficking and smuggling-and to develop effective responses in advance. The use of such simulations facilitates optimal resource allocation, enhanced emergency preparedness, and improved coordination between national services. The scalability and adaptability of digital twins enable modeling of various terrain types in the region: the river and maritime borders of Romania, the forested and mountainous areas of the Carpathian Mountains in Moldova and Ukraine, and steppe and border zones. Digital twins integrate a variety of geospatial data, including digital surface models (DSMs), hydrological data, satellite imagery, and transport infrastructure information. This data creates dynamic multidimensional representations that simulate real-world conditions, assess border permeability, and optimize surveillance strategies. Particular attention is paid to the region's natural and infrastructural features: the depth and flow velocity of the Prut and Danube rivers, seasonal ice conditions, forest density, road network quality, and the remoteness of settlements. Digital twins enable forecasting how these factors impact the movement of people and equipment and developing measures to improve border control efficiency. In the context of the Smart Border, this technology becomes a key tool for integrating national situational images into

regional models, increasing interoperability with EU systems, and coordinating efforts between Romania, Moldova, and Ukraine.

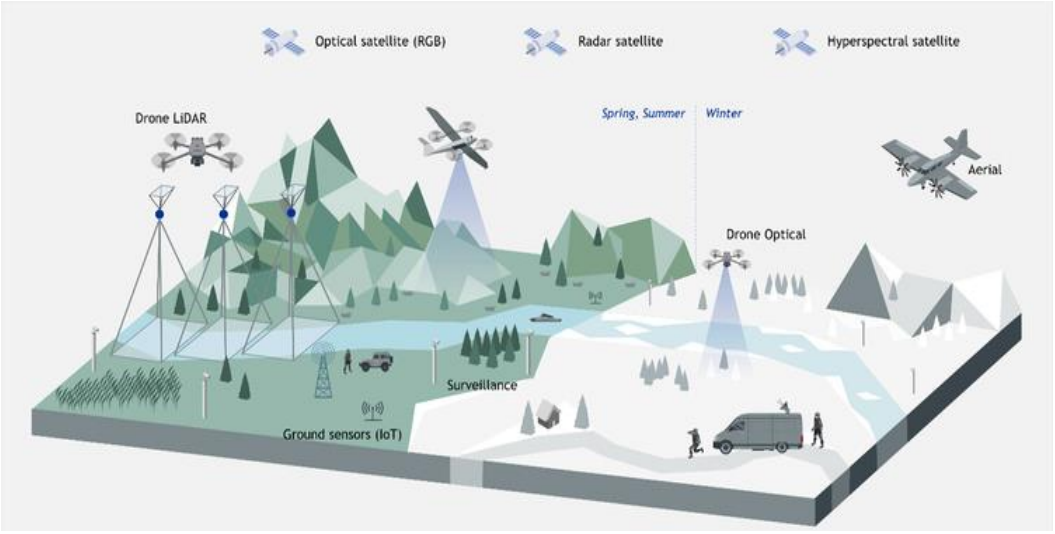

Fig. 5. A visual representation of a digital twin of a border region [21].
Source: Frontex

5.2 Adaptation of ESRI tools for coordination of national and regional situational maps
Effective border and defense infrastructure management requires the integration of diverse information flows and analytical systems. One of the key elements of a modern approach to security management is the use of geographic information systems (GIS) and analytical platforms, such as ESRI tools, which enable the creation of dynamic situational maps at the national and regional levels.

In the context of regional integration, Esri's ArcGIS platform can be considered a promising technological component of the "smart border" infrastructure along the Romania-Moldova-Ukraine axis. As a reminder, on December 20, 2019, Esri signed a four-year general management agreement (GMA) with the European Commission for the provision of licenses and support for its products. Although the agreement formally expired in December 2023, its existence demonstrates the EU's level of trust in the platform and facilitates access for countries-partners to similar solutions. When adapting this platform to the needs of the region's border management, it is important to consider:

- the need to purchase licenses or conclude framework agreements at the national level in each country;
- requirement for integration with open geospatial data standards (e.g. INSPIRE Directive) and NATO standards (STANAG, AJP) to ensure interoperability;
- the importance of localization, user training, and providing support through regional distributors and service-Esri partners.

Thus, using Esri-instruments should not be seen as the only way, but as a strategic option that fits optimally into the dual-use (civil and defense) system, subject to proper licensing, adaptation and integration at the national and regional level.

5.3 Technical capabilities and potential

Esri ArcGIS tools provide a wide range of functionality suitable for smart border infrastructures, enabling the collection and integration of data from various sources - border sensors, satellite platforms, drones, and law enforcement or defense databases. Furthermore, the platform offers analytical modules based on artificial intelligence and machine learning that can identify threat patterns, predict risks, and model crisis response scenarios. Real-time visualization of information, including maps of high-risk areas, migration, and logistics flows, is made possible by Esri integration - Data infrastructure solutions at the national and regional levels. Finally, the platform's high degree of interoperability - in particular, its support for the EU Open Data Directive and the ability to synchronize with European and NATO systems - makes it suitable for coordination between countries in the region and European initiatives.

5.4. Adaptation for Moldova, Romania and Ukraine and links with EU programmes in the context of the TEN-T Digital Transport Corridors and the Defence Roadmap to 2030

In the context of the Romania-Moldova-Ukraine axis, the adaptation of Esri ArcGIS platforms and other geoinformation solutions is of strategic importance in the implementation of both TEN infrastructure corridors-T, and the activities of the Roadmap for Ensuring Defense Capability by 2030. TEN Corridors-Multimodal transport networks (road, rail, inland waterways, and maritime routes) facilitate civilian and military flows, and digital support for these networks through situational maps, monitoring, and analysis is becoming key. At the same time, the Preserving Peace Defense Readiness Roadmap 2030 program identifies the need to create a "military mobility area" network with harmonized rules and logistics routes by 2027. Therefore, the integration of GIS solutions at the level of Romania, Moldova, and Ukraine must consider two parallel contexts: trans-European transport infrastructure and defense mobility. This means not simply installing platforms, but adapting them to national legal frameworks, integrating with open standards (INSPIRE), and socializing processes with academic and industrial technology partners. This synchronization ensures data and management continuity in transport and logistics corridors, which simultaneously serve civilian and defense purposes, and strengthens the region's strategic resilience.

6. Conclusions and recommendations

6.1. Conclusions

1. The implementation of the concepts of “Smart borders” and digital corridors on the Romania-Moldova-Ukraine axis creates a new paradigm of security and sustainable mobility, where civilian and military flows are integrated into one information system-analytical system.
2. Integration of NATO standards (STANAG, AJP) and the INSPIRE Directive ensures interoperability of geospatial data and strengthens situational awareness between countries in the region.

3. The architecture of digital corridors and HNS (Host–Nation Support) systems is a key element in the implementation of the Defence Readiness Roadmap 2030 strategic document presented by the European Commission on 16 October 2025.

4. GIS and AI Tools-Analytics and digital twins provide the foundation for coordinating transport, logistics, and border flows, including TEN-T programs and activities for visualizing the situational picture.
5. The participation of academic institutions and private companies enhances the region's innovative potential, creating a dual-use ecosystem-use), where technologies are developed and commercialized to achieve security and economic development.

6.2. Recommendations

1. Harmonization of regulatory frameworks and data standardization. Countries in the region are encouraged to adapt national legislation and data exchange protocols to NATO and EU standards, including metadata and formats (STANAG 7074, INSPIRE), as soon as possible.
2. Develop digital border management infrastructure. Ensure the implementation of GIS-platforms and digital twins adapted to the specific features of the region (rivers, topography, transport corridors), with an emphasis on linking with TEN systems-T and the Military Mobility strategy.
3. Investment in human resources and Academic-Industrial partnerships. Create regional centers of excellence, joint university-industry labs, train specialists in AI, cybersecurity, and geoanalytics, and stimulate startups and dual-use enterprises.
4. Accelerate the implementation of the roadmap by 2030. Implement four priority projects (Counter-UAS, Eastern Flank Surveillance, European Air Shield, European Space Shield) taking into account the regional logic of the Romania-Moldova-Ukraine axis and linking to digital corridors.
5. Develop monitoring and evaluation mechanisms. Develop a system of key performance indicators (KPIs) to assess smart border implementation, data interoperability, response times, and compliance with the Readiness 2030 roadmap.
6. Financing and resourcing. Use resources from EU initiatives (EDIP, SAFE, Horizon Europe) and national funds to finance security and digitalisation infrastructure, ensuring long-term sustainability and independence of the technology chain [22].

6.3. Conclusion

The digital transformation of security and defense systems is an integral element of modern public policy. The use of GIS, AI, and integration platforms allows countries on Europe's eastern flank to strengthen their resilience, improve decision-making efficiency, and integrate into European initiatives. The 2030 Defense Roadmap serves as a guide for coordinated action at the national and regional levels, while the implementation of advanced technologies and innovative ecosystems ensures long-term strategic potential. The comprehensive application of these measures creates conditions for the eastern flank not only to protect its borders but also to actively contribute to Europe's overall defense by building a sustainable, technologically independent, and secure regional infrastructure.

References

[1] EU Commission, Military Mobility 2.0, "Military Mobility: EU proposes actions to," 2022. [Online Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6583.

[2] EU Commission, "Migration and Home Affairs," Smart borders, 2022. [Online]. Available: https://home.

[3] UK Government, "Allied Joint Doctrine for Host-Nation Support (AJP-4.3)," 2021. [Online]. Available https://www.gov.uk/government/publications/allied-joint-doctrine-for-host-nation-supportajp-43a.

[4] A. Babin, S. Tutunaru and I. Covalenco, "TEN-T digital transport corridors in the Republic of Moldova achievements and perspectives," *Smart Urban Development - Dezvoltare Urbană Inteligentă,* pp. 13-33 2025.

[5] NATO, STANAG (Standardization Agreement), "Standardization," 2021. [Online]. Available https://www.nato.int/cps/cn/natohq/topics_69269.htm.

[6] NATO, USA, Joint Chiefs of Staff (CJCS), "Allied joint doctrine and assists in NATO," 2025. [Online Available: https://www.jcs.mil/Doctrine/Joint-Allied-Doctrine-Program/.

[7] EU Commission, "INSPIRE Knowledge base," INSPIRE Directive, 2007. [Online]. Available https://knowledge-base.inspire.ec.europa.eu/legislation/inspire-directive_en.

[8] EU Commission, "Mobility and Transport," TEN-T Regulation, 2024. [Online]. Available https://transport.ec.europa.eu/transport-themes/infrastructure-and-investment/trans-european.

[9] EU Commission, "Migration and Home Affairs," European Border Surveillance system (EUROSUR 2013. [Online]. Available: https://home-affairs.ec.europa.eu/policies/schengen/eurosur_en.

[10] EU Commission, Horizon 2020, "Architecture for EuroOpean Logistics Information exchange," [Online Available: https://cordis.europa.eu/project/id/690797.

[11] EU, "European Federated Network of Information eXchange in LogistiX," [Online]. Available https://fenix-network.eu/.

[12] STANAG 7074, "Digital Geographic Information Exchange Standard (DIGEST)," [Online]. Available https://proceedings.esri.com/library/userconf/europroc98/proc/idp29.html.

[13] EU Commission Directorate-General for Communication, "How the new digital borders," 2025. [Online Available: https://commission.europa.eu/news-and-media/news/how-new.

[14] EU Commissio, "Migration and Home Affairs," Interoperability Framework for Border and Security Dat Systems, [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/fr/memo_17_5241.

[15] European Union, "Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 2 October 2013 establishing the European Border Surveillance System (Eurosur)," [Online]. Available https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R1052.

[16] EU Commission, "Commission Implementing Regulation (EU) 2021/581 of 9 April 2021 on the situational pictures of the European Border Surveillance System (EUROSUR)," [Online]. Available: https://eur lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:32021R0581&qid=1618306409753.

[17] EU Commission, "Frontex," GIS for Border Management and Surveillance, [Online]. Available https://www.esri.com/~/media/files/pdfs/events/gis%20in%20the%20eu/filipe%20paisana20frontex_locked%20presentation02.pdf.

[18] EU Commission, "Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR) [Online]. Available https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2011:1536:FIN:EN:PDF.

[19] EU, Frontex, "European Border and Coast Guard Agency, "Artificial intelligence based capabilities for the European Border and Cast Guard" (Final report)," [Online]. Available https://www.frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_020_final_report.pdf.

[20] EU, JOINT COMMUNICATION TO THE EU PARLIAMENT, THE EU COUNCIL AND TH COUNCIL, "Preserving Peace - Defense Readiness Roadmap 2030," 2025. [Online]. Availabl https://defence-industry-space.ec.europa.eu/eu-defenceindustry/readiness-roadmap-2030_en .

[21] EU, Frontex, the European Border and Coast Guard Agency, "Research and Innovation," 2025. [Online Available: https://www.frontex.europa.eu/innovation/research-and-innovation/prize-contests/prizeawar contest-on-copernicus-border-surveillance-service-evolution-CczoJ8.

[22] European Council, "European Council conclusions on defense, European defense industry program [Online]. Available: https://www.consilium.europa.eu/en/policies/european-defence-readiness/.