Cybersecurity Challenges in Digital Logistics Systems of the East-West Transport Corridor

Khayala Ibrahimova[1][0000-0002-8380-9117] , Sabina Naghiyeva[2][0009-0001-3521-088X] and Afsana Gulieva[3][0009-0004-2388-562X]

Baku Engineering University, Khirdalan 120 AZ0101, Azerbaijan

Abstract. This article analyzes cybersecurity challenges arising in digital logistics systems operating within the framework of the East–West Transport Corridor. In recent years, the widespread adoption of IoT technologies, cloud-based platforms, and real-time data exchange systems in the logistics sector has significantly enhanced operational efficiency, transparency, and managerial flexibility. However, the increasing reliance on digital infrastructure has simultaneously rendered these systems more vulnerable to diverse and increasingly sophisticated cyber threats. In particular, ransomware attacks, data breaches, supply chain attacks, DDoS attacks, and intrusions targeting industrial control systems pose serious risks to the resilience and uninterrupted operation of logistics infrastructure. This study identifies key challenges, including the disparity in cybersecurity maturity levels among countries participating in the East–West Corridor, the absence of unified security standards, the continued use of legacy systems, and risks associated with cross-border data exchange. The article systematically analyzes existing vulnerabilities and evaluates their potential impact on operational continuity, data integrity, confidentiality, and overall economic stability.
Furthermore, a comprehensive security framework is proposed, integrating Zero Trust architecture, AI-based anomaly detection systems, SIEM integration, blockchain-based tracking mechanisms, and internationally coordinated cybersecurity strategies. The findings indicate that without the implementation of a unified, multi-layered, and proactive approach, ensuring the long-term security and resilience of digital logistics systems will not be feasible.

Keywords: Cybersecurity, Digital Logistics Systems, East-West Transport Corridor, Supply Chain Security, Internet of Things (IoT) Security, Ransomware Attacks, SCADA and Industrial Control Systems Security, Zero Trust Architecture, Security Information and Event Management (SIEM), Cross-border Data Security.

1 Introduction

In the last decade, the ongoing digitalization of global trade and transportation ecosystems has significantly transformed the operational paradigms of the logistics sector. The integration of advanced technologies—such as the Internet of Things (IoT), cloud computing infrastructures, big data analytics, and real-time monitoring solutions—has

enabled more adaptive, data-driven, and efficient logistics management processes. These innovations have enhanced decision-making capabilities throughout the supply chain while contributing to cost optimization and improved operational transparency. Nevertheless, the expansion of digital infrastructures has concurrently increased exposure to cyber threats and system vulnerabilities [12], [15].

Within this context, the deployment of digital logistics systems across transnational and strategically critical transportation networks, including the East–West Transport Corridor, introduces a distinct set of cybersecurity concerns [16]. As a major trade linkage between Europe and Asia, this corridor operates across diverse national environments characterized by varying levels of technological advancement, regulatory frameworks, and cybersecurity readiness. Such heterogeneity directly influences the overall robustness and resilience of the integrated logistics ecosystem [2].

Moreover, digital logistics infrastructures have become increasingly attractive targets for a wide spectrum of cyber threats, including ransomware incidents, phishing schemes, data exfiltration, distributed denial-of-service (DDoS) attacks, and intrusions into industrial control systems such as SCADA and ICS environments. The consequences of these attacks extend beyond technical disruptions, often resulting in substantial financial losses, operational inefficiencies, and interruptions in international supply chain continuity. In addition, the growing reliance on cross-border data exchange and interoperable digital platforms further amplifies the complexity of the cybersecurity landscape [3], [4], [5].

Although prior studies have predominantly examined the security implications of isolated technologies or region-specific logistics systems, there remains a notable lack of comprehensive research addressing cybersecurity risks within fully integrated, multi-country logistics networks. This limitation is particularly pronounced in geopolitically and economically significant corridors with heterogeneous infrastructures, such as the East–West Transport Corridor [13], [15].

Accordingly, this study aims to provide a systematic analysis of the cybersecurity challenges affecting digital logistics systems operating within the East–West Transport Corridor, identify critical vulnerabilities, and propose integrated, practical, and scalable security strategies to mitigate emerging risks.

2 Problem Statement

The ongoing process of digital transformation has profoundly redefined the logistics industry, reshaping traditional supply chain management into a more interconnected, automated, and real-time-oriented system. The integration of Internet of Things (IoT) technologies, the expansion of cloud computing infrastructures, the application of big

data analytics, and the intensification of data exchange across multiple digital platforms have collectively enhanced the efficiency and responsiveness of logistics operations. At the same time, these developments have significantly broadened the cybersecurity attack surface, giving rise to more sophisticated and evolving threat vectors [12], [15]. These risks become particularly pronounced in transnational, strategically significant, and highly integrated logistics networks such as the East–West Transport Corridor. As this corridor links regions with differing levels of technological advancement, the resulting digital ecosystem is inherently heterogeneous. Variations in cybersecurity maturity, regulatory frameworks, and technical capabilities among participating countries contribute to structural imbalances, creating potential "weak points" that can undermine the overall security resilience of the system [2], [16].

In addition, the lack of harmonized and standardized cybersecurity frameworks further exacerbates vulnerabilities associated with cross-border data exchange. The increasing volume of data flows, coupled with the reliance on interoperable platforms and real-time coordination mechanisms, creates favorable conditions for a wide range of cyber threats, including ransomware attacks, phishing campaigns, supply chain compromises, distributed denial-of-service (DDoS) attacks, and intrusions targeting industrial control environments such as SCADA and ICS systems [3], [10]. These threats extend beyond information security concerns, posing serious risks to the continuity and stability of physical logistics operations.

Although existing studies have largely concentrated on the protection of individual technologies or localized logistics environments, there is a noticeable lack of comprehensive and integrated analyses addressing cybersecurity challenges in multi-country logistics corridors. This research gap is particularly evident in geostrategically critical infrastructures such as the East–West Transport Corridor, where diverse legal systems, technological ecosystems, and operational practices intersect.

This study addresses the fundamental challenge that, despite the high level of integration in modern digital logistics systems, there is still no unified, adaptive, and real-time-oriented cybersecurity architecture capable of ensuring their resilience. This limitation increases exposure to risks affecting operational continuity, data integrity, confidentiality, and broader regional economic stability. Consequently, the development of coordinated, multi-level cybersecurity strategies—encompassing both technical and institutional dimensions—has become an essential requirement.

3 System Architecture, Security Analysis and Discussion

This section provides a detailed examination of the system architecture and the corresponding cybersecurity challenges inherent in digital logistics environments. It opens with an overview of digital logistics systems, emphasizing their growing dependence on interconnected technologies and data-centric operational models. The analysis then addresses the evolving cybersecurity threat landscape, focusing specifically on vulnerabilities within critical transportation infrastructures such as the East–West Transport Corridor. In this context, Azerbaijan's role as a strategic transit hub is considered from both regional and international security perspectives. The section further assesses the

potential operational and economic consequences of cyber incidents in logistics systems. Finally, a structured cybersecurity framework is introduced, presenting practical and scalable mitigation strategies aimed at strengthening system resilience and ensuring secure, sustainable logistics operations.

3.1 Overview of Digital Logistics Systems

Digital logistics systems have emerged as a fundamental component of contemporary global supply chain management, driving a transition from traditional, static models toward dynamic, real-time, and data-driven operational environments. Through the integration of advanced digital technologies, logistics processes are now continuously monitored, analyzed, and optimized, resulting in increased efficiency, responsiveness, and transparency across supply chains.

At the core of these systems are Internet of Things (IoT) technologies, which enable real-time tracking and monitoring of logistics assets. IoT devices collect and transmit data related to vehicle positioning, cargo conditions, temperature, humidity, and other critical variables. This continuous data flow allows logistics operators to improve decision-making accuracy, minimize delays, and optimize resource allocation. In parallel, the integration of GPS and sensor-based technologies enhances visibility throughout the entire logistics chain, supporting end-to-end transparency in cargo movement [7], [15].

Cloud computing platforms represent another essential pillar of digital logistics infrastructures. By enabling centralized data storage and distributed processing across geographically dispersed logistics nodes, cloud-based systems support real-time data analytics and accelerate decision-making processes. Additionally, these platforms facilitate seamless data exchange among multiple stakeholders, thereby improving coordination and strengthening the integration of global logistics networks [6], [7].

Big Data analytics and Artificial Intelligence (AI) technologies further enhance the capabilities of digital logistics systems by enabling predictive and adaptive operations. These technologies are widely utilized for demand forecasting, route optimization, risk assessment, and cost reduction [12], [14]. AI-driven solutions also contribute to anomaly detection and decision-support systems, allowing logistics operations to respond more effectively to dynamic and uncertain environments.

In addition, blockchain technology has been increasingly adopted in certain logistics applications to ensure data integrity, transparency, and trust across supply chains. Its decentralized and immutable structure makes it particularly suitable for enhancing product traceability, digitizing documentation workflows, and reducing the risk of fraud.

However, the growing integration of these diverse technologies has resulted in highly complex, multi-layered system architectures. Modern digital logistics ecosystems consist of numerous interconnected components, platforms, and service providers, all engaged in continuous data exchange. While such integration significantly improves operational efficiency, it also increases system complexity and introduces additional challenges in terms of system management and security [2], [7].

These challenges become even more pronounced in multi-country logistics frameworks such as the East–West Transport Corridor. Variations in technological development, inconsistencies in standards, and disparities in digital infrastructure across participating countries complicate the establishment of a unified and fully integrated logistics ecosystem. As a result, despite their high performance and strategic importance, these systems require advanced coordination mechanisms and more sophisticated management approaches.

In summary, digital logistics systems play a critical role in enhancing the efficiency and effectiveness of global supply chains. Nevertheless, their increasing technological complexity and level of integration also give rise to new categories of cybersecurity and governance challenges that must be addressed to ensure long-term resilience and sustainability.

3.2 Cybersecurity Threat Landscape in Logistics

Digital logistics systems constitute highly integrated and multi-layered information environments that are central to modern supply chain operations. These systems rely on continuous data exchange across IoT devices, cloud infrastructures, API-based integrations, GPS tracking technologies, and various third-party service providers. While this level of interconnectivity enhances efficiency and operational coordination, it simultaneously broadens the attack surface, resulting in a more complex and multi-dimensional cybersecurity threat environment.

Among the most significant threats facing the logistics sector are ransomware attacks, which are specifically designed to encrypt critical systems and disrupt operational continuity. Key components such as port management platforms, Warehouse Management Systems (WMS), and transportation planning systems are particularly susceptible. The impact of such incidents extends beyond data loss, often causing severe interruptions in physical logistics processes and generating substantial financial losses [4], [5].

Another critical category of threats is supply chain attacks, which are typically more sophisticated and harder to detect. Rather than targeting primary systems directly, these attacks exploit vulnerabilities in software dependencies, update channels, or third-party service providers. As a result, even trusted components within the system can become compromised, potentially triggering large-scale and cascading security failures.

Human-centered attack vectors, including phishing, spear-phishing, and credential harvesting, also represent a major risk. Personnel involved in logistics operations—such as system administrators and coordination staff—are frequently targeted to gain unauthorized access. Successful exploitation can lead to data manipulation, privilege escalation, and even deliberate disruption of operations. This highlights the persistent role of human factors as a critical vulnerability within digital logistics ecosystems [6], [11].

In addition, Distributed Denial of Service (DDoS) attacks pose a significant threat to the availability of logistics platforms. Such attacks can interrupt real-time operations, which are essential for functions such as cargo tracking, route optimization, and system

coordination. Given the time-sensitive nature of logistics processes, even short-term service disruptions can result in considerable operational and economic consequences.

A more advanced attack surface is associated with Industrial Control Systems (SCADA/ICS) and IoT-based sensor networks. Compromises within these environments can have direct physical implications, affecting not only digital data but also real-world logistics operations. For instance, attackers may manipulate cargo routing, alter environmental control parameters such as temperature, or disrupt automated warehouse processes.

Furthermore, sophisticated threat categories such as zero-day exploits and Advanced Persistent Threats (APT) are becoming increasingly relevant in the logistics domain. These attacks typically involve prolonged, stealthy infiltration strategies that enable deep system compromise and are often difficult to detect using conventional security tools [6], [10].

In summary, the cybersecurity threat landscape in digital logistics systems is inherently complex, dynamic, and continuously evolving. The coexistence of technical vulnerabilities and human-related risks demonstrates the limitations of traditional reactive security models. Consequently, there is a critical need for adaptive and proactive security approaches, including real-time monitoring, behavior-based anomaly detection, and the implementation of integrated, multi-layered security architectures.

3.3 Vulnerabilities in the East-West Transport Corridor

The East–West Transport Corridor represents a strategically significant multimodal logistics network linking Europe and Asia, integrating the transport, information, and communication infrastructures of multiple countries into a complex ecosystem. Beyond the physical movement of goods, the corridor also facilitates real-time data flows through digital logistics platforms, resulting in a highly interdependent and sensitive structure across both physical and cyber domains.

The East–West Transport Corridor constitutes a strategically critical, multimodal logistics network that connects Europe and Asia by integrating transportation, information, and communication infrastructures across multiple countries. In addition to facilitating the physical movement of goods, the corridor supports continuous real-time data exchange through digital logistics platforms, resulting in a highly interconnected and interdependent ecosystem spanning both physical and cyber domains.

One of the primary vulnerabilities of this multi-national architecture lies in the uneven distribution of cybersecurity maturity among participating countries. Differences in levels of digital transformation, security standards, and technological capabilities hinder the development of a unified and cohesive defense framework. As a consequence, the overall security posture of the corridor is often determined by its least secure component, reflecting a classic “weakest link” phenomenon [4], [8].

The lack of a standardized and harmonized security architecture further intensifies systemic risks. The coexistence of diverse network protocols, authentication methods, and data management practices complicates the implementation of consistent security controls across the ecosystem. While such heterogeneity may support interoperability

to some extent, it simultaneously creates fragmented entry points that expand the attack surface and increase the likelihood of large-scale system compromise.

Another significant source of vulnerability is the continued reliance on legacy systems within certain segments of the corridor. These outdated technologies frequently fail to meet contemporary cybersecurity requirements and often lack essential protections such as robust encryption, multi-factor authentication, and real-time threat detection capabilities. As a result, they function as high-risk nodes that can be exploited by adversaries [3], [7], [9].

Cross-border data exchange introduces additional layers of complexity due to both legal and technical fragmentation. Variations in data governance policies across jurisdictions lead to inconsistencies in data protection, storage, and transmission practices, thereby increasing the risk of data breaches and operational inefficiencies. In particular, inadequately secured API integrations serve as critical vulnerability points within the system.

Substantial disparities are also evident in the underlying network infrastructure. While some regions benefit from high-speed, encrypted, and continuously monitored networks, others rely on less developed and insufficiently secured systems. This imbalance limits the implementation of unified security measures such as end-to-end encryption and centralized monitoring, ultimately reducing visibility and control over real-time logistics operations.

In addition to technical factors, human and organizational dimensions play a crucial role in shaping the overall risk landscape. Inconsistent cybersecurity training, the absence of standardized incident response frameworks, and limited awareness among personnel increase susceptibility to social engineering attacks, particularly phishing and credential-based exploitation.

Furthermore, the strong reliance on third-party vendors and external service providers significantly amplifies exposure to supply chain attacks. Given the extensive use of external software solutions, cloud infrastructures, and API-driven services within logistics systems, such attacks are not only more probable but also more challenging to detect at early stages [3], [12].

In conclusion, cybersecurity vulnerabilities within the East–West Transport Corridor are inherently multidimensional, encompassing technical, organizational, legal, and infrastructural aspects. Effectively mitigating these risks requires not only advanced technological solutions but also coordinated cross-border strategies, the development of standardized security frameworks, and the implementation of continuous, real-time monitoring mechanisms.

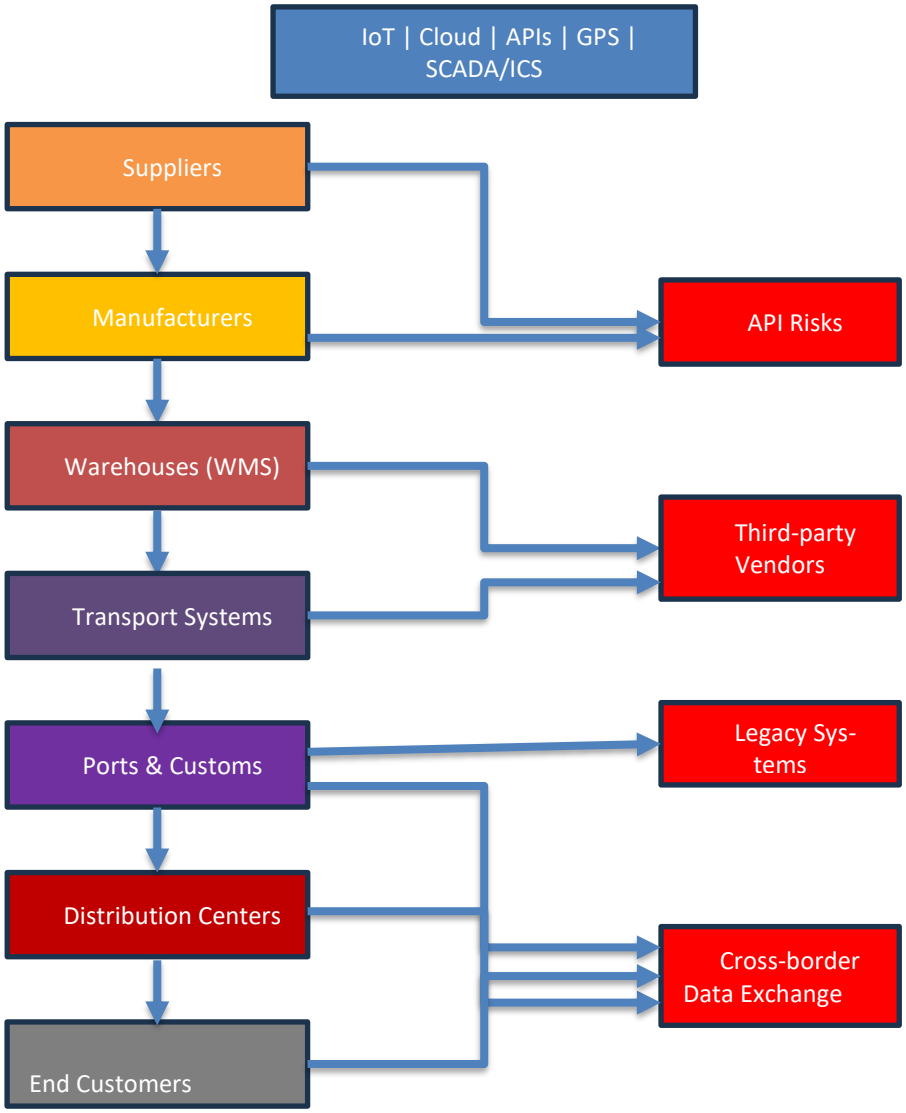

Figure 1. Architecture of Digital Logistics Systems and Associated Cyber Risk Points

3.4 Azerbaijan as a Critical Transit Node in the Corridor

Azerbaijan occupies a pivotal position within the East–West Transport Corridor, functioning as a strategic transit hub that connects Europe and Asia while ensuring the continuity of regional supply chain operations. Its advantageous geographical location, direct access to the Caspian Sea, and ongoing development of multimodal transport infrastructure have established the country as a central node in international logistics

networks. Key assets such as the Baku International Sea Trade Port, the Alat Free Economic Zone, and the expanding railway system have collectively strengthened Azerbaijan's role as a major logistics and distribution center, where advanced digital logistics solutions are actively deployed.

In recent years, the country has undergone a rapid digital transformation in the transportation and logistics sector. Technologies such as IoT-based monitoring systems, GPS tracking solutions, cloud computing platforms, and data analytics tools are increasingly utilized for cargo management, real-time tracking, route optimization, and warehouse automation. These advancements have significantly enhanced operational efficiency and enabled more agile, data-driven decision-making processes. At the same time, they have introduced a more complex, multi-layered cybersecurity environment, particularly in relation to critical infrastructure systems [6], [7].

Azerbaijan's strategic transit role also elevates its profile as a high-value target in the cybersecurity domain. Data flows traversing the country are not limited to national operations but are integral to the broader Europe–Asia logistics ecosystem. Consequently, cyber incidents within Azerbaijan's logistics infrastructure may have cascading effects, leading to disruptions not only at the national level but also across regional and global supply chains. This strategic importance increases the likelihood of targeting by both state-sponsored actors and financially motivated cybercriminal groups.

Moreover, the country's integration into international logistics networks necessitates extensive reliance on API-based data exchange, third-party service providers, and cloud-based logistics management systems. While these integrations enhance interoperability and operational efficiency, they simultaneously introduce additional attack vectors, particularly at the supply chain level. Variations in the cybersecurity maturity of external vendors and the lack of fully standardized security practices across interconnected systems further amplify these risks [3], [7], [11].

The deployment of Industrial Control Systems (ICS), SCADA infrastructures, and IoT-based sensor networks within Azerbaijan's logistics ecosystem highlights the convergence of physical and digital domains. This interconnection creates scenarios in which cyberattacks can directly impact physical operations. For example, unauthorized manipulation of port management systems, disruption of automated warehouse processes, or misrouting of cargo shipments can lead to significant operational and financial consequences [2], [6].

Additionally, Azerbaijan's role as a transit hub intensifies the volume of cross-border data exchange, thereby increasing the complexity of data governance and regulatory compliance. Real-time data transmission across multiple jurisdictions introduces challenges related to inconsistencies in legal frameworks, technical standards, and cybersecurity protocols. Such discrepancies can elevate the risk of data exposure and leakage [9], [16].

At the same time, Azerbaijan's strategic position underscores the importance of international cooperation and coordinated cybersecurity efforts. The absence of mechanisms for real-time threat intelligence sharing, harmonized security standards, and cross-border incident response can significantly weaken overall system resilience. In this regard, Azerbaijan has the potential not only to serve as a transit country but also to evolve into a regional hub for cybersecurity coordination and collaboration.

In conclusion, Azerbaijan's role as a critical transit node within the East–West Transport Corridor elevates the cybersecurity of its digital logistics infrastructure to a strategic priority. The effectiveness of security measures implemented in this context has direct implications not only for national infrastructure protection but also for the stability, continuity, and resilience of the broader regional logistics ecosystem.

3.5 Impact of Cyber Attacks on Logistics Operations

Cybersecurity incidents in digital logistics systems extend far beyond isolated technical disruptions; they represent complex events that generate interconnected impacts across operational, economic, and geopolitical dimensions. In large-scale, multi-country logistics networks such as the East–West Transport Corridor, these effects are significantly amplified, posing direct threats to the stability and integrity of regional supply chains.

The most immediate and critical consequence is the disruption of operational continuity. Cyber incidents—including ransomware attacks, Distributed Denial of Service (DDoS) attacks, and unauthorized access to critical systems—can lead to partial or complete outages of port management platforms, customs information systems, and cargo planning applications. Such disruptions often result in container congestion, delays in transportation schedules, and bottlenecks across logistics networks. Due to the interconnected nature of these systems, failures originating at a single node can rapidly propagate, triggering cascading or domino effects throughout the entire corridor [3], [4], [6].

A second major dimension of impact relates to economic losses. In logistics operations, where time efficiency is directly linked to cost, even short-term disruptions can generate substantial financial consequences. Delayed deliveries may incur contractual penalties, while additional costs arise from extended warehousing, rerouting of shipments, and operational rescheduling. Furthermore, data breaches involving sensitive commercial or customer information can result in legal liabilities, reputational damage, and long-term reductions in competitive positioning [7], [11].

Another critical impact concerns the degradation of data integrity and the resulting decline in decision-making accuracy. Digital logistics systems are heavily dependent on real-time data streams; therefore, any manipulation, corruption, or inconsistency in data can lead to flawed operational decisions. This may manifest in misrouted cargo, inaccurate inventory management, and discrepancies in customs documentation. Beyond immediate disruptions, such scenarios create a "distorted information environment," which introduces systemic risks that are often more difficult to detect and mitigate.

Cyber incidents also contribute to increased systemic fragility within supply chain ecosystems. Modern logistics infrastructures rely extensively on interconnected components, including third-party service providers, API-based integrations, and cloud platforms. A security compromise within a single element can propagate across the network, leading to widespread disruption. This cascading failure dynamic is particularly critical in integrated regional corridors, where operational dependencies span multiple countries and jurisdictions.

In addition to operational and economic consequences, cybersecurity incidents carry strategic and geopolitical implications. As the East–West Transport Corridor functions as a vital alternative route for international trade, significant disruptions may influence global trade patterns, reduce stakeholder confidence, and elevate the political sensitivity of logistics infrastructures. In this context, cybersecurity emerges not only as a technical concern but also as a key factor in economic diplomacy and international stability.

Another important long-term effect is the erosion of trust in digital transformation initiatives. Recurrent cyber incidents may undermine confidence in cloud-based infrastructures, automated logistics systems, and real-time monitoring technologies. This loss of trust can slow the adoption of innovative solutions and potentially drive organizations toward more conservative, less efficient operational models, thereby hindering overall digital progress [6], [11].

In summary, the impacts of cyberattacks on logistics operations are multidimensional and extend well beyond the boundaries of information systems. They simultaneously affect operational continuity, financial performance, data reliability, and geopolitical stability. Accordingly, cybersecurity in digital logistics environments should be recognized not merely as a protective measure, but as a fundamental component of strategic resilience and sustainable system design.

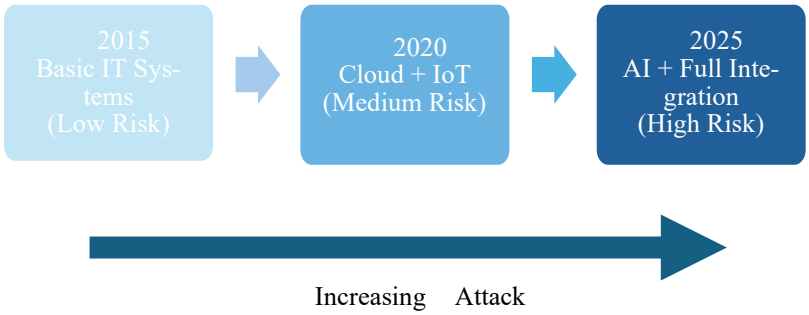

Figure 2. Growth of Cyber Attack Surface in Digital Logistics Systems (2015–2025)

Case Study: Ransomware Attack on a Regional Logistics Network

A significant ransomware incident targeted a regional logistics operator operating within a transnational transport corridor. The attack originated from a phishing email that successfully compromised employee credentials, granting the threat actors initial access to the internal network.

Once inside, the attackers conducted lateral movement across interconnected systems, exploiting weak network segmentation and legacy infrastructure components. Critical logistics platforms—including Warehouse Management Systems (WMS), transport scheduling platforms, and customs data exchange interfaces—were encrypted, resulting in severe operational disruptions.

Operational Impacts:

- Temporary suspension of port operations

- Unavailability of cargo tracking systems
- Disruption of cross-border shipment coordination

Consequential Outcomes:

- Substantial delays in cargo delivery
- Financial losses stemming from operational downtime
- Compromise of data integrity and loss of stakeholder trust

Identified Security Gaps:

- Incomplete implementation of Multi-Factor Authentication (MFA)
- Lack of real-time anomaly detection within security monitoring systems
- Insufficiently secured access points for third-party vendors

This case illustrates the potential for ransomware attacks to propagate through highly interconnected logistics ecosystems, triggering cascading failures across multiple countries within a transport corridor. It underscores the necessity for robust, multi-layered cybersecurity measures, including stringent access controls, real-time monitoring, and comprehensive vendor risk management, to safeguard critical regional logistics operations.

Threat Type	**Impact on Logistics**	**Mitigation Strategy**
Ransomware	System shutdown, operational disruption	Backup systems, network segmentation, Zero Trust
Phishing / Credential Theft	Unauthorized access, data breach	MFA, user awareness training
Supply Chain Attack	Compromise via third-party vendors	Vendor risk management, security audits
DDoS	Service unavailability	Traffic filtering, load balancing
IoT/ICS Attacks	Physical process manipulation	Device authentication, network isolation
Data Breach	Loss of confidentiality, legal issues	Encryption, DLP systems
APT (Advanced Persistent Threat)	Long-term hidden compromise	AI-based anomaly detection, SIEM/SOAR

Table 1. Mapping of Cyber Threats to Operational Impacts and Mitigation Strategies in Digital Logistics Systems

3.6 Proposed Cybersecurity Framework and Mitigation Strategies

The increasing complexity of digital logistics systems within the East–West Transport Corridor, coupled with exposure to multi-layered cyber threats, highlights

the insufficiency of traditional reactive security approaches. This necessitates an integrated, proactive, and risk-oriented cybersecurity framework to ensure resilience across physical and digital domains.

At the core of the proposed framework is the Zero Trust Architecture (ZTA). In this model, the conventional principle of "trust but verify" is replaced with continuous verification: every user, device, and system component undergoes ongoing authentication and risk assessment. Micro-segmentation further restricts lateral movement within the network, which is critical for logistics environments spanning multiple transit countries with extensive third-party integrations [1], [6], [7].

The second pillar integrates Security Information and Event Management (SIEM) with Security Orchestration, Automation, and Response (SOAR) systems. SIEM continuously collects and correlates log data, while SOAR enables automated responses based on detected anomalies. This integration accelerates detection and mitigation processes, reducing the Mean Time to Respond (MTTR) [6], [11].

The third component leverages AI/ML-based behavioral analytics and anomaly detection. Unlike traditional rule-based systems, these tools construct dynamic behavioral baselines for cargo flows, device activity, API requests, and user interactions. Deviations from baseline patterns trigger real-time alerts, enabling adaptive threat detection.

The fourth element employs the Defense-in-Depth strategy, providing layered protection across networks, applications, data, and physical infrastructure. For example, firewalls and intrusion detection systems safeguard network layers, while encryption and Data Loss Prevention (DLP) tools secure sensitive data.

A supply chain cybersecurity governance framework is also essential. Security standards should be enforced for all third-party vendors, with periodic risk audits and compliance monitoring against international benchmarks such as ISO/IEC 27001. Vendor Risk Management (VRM) tools can assess the security maturity of ecosystem partners [3], [9], [11].

At the regional level, cross-border Cyber Threat Intelligence (CTI) sharing platforms are recommended to facilitate real-time information exchange among corridor countries. This enables early attack detection and coordinated defensive strategies.

Infrastructure-level measures include IoT security hardening, secure firmware updates, device identity management, and encrypted communication protocols (e.g., TLS 1.3, IPsec). For SCADA and ICS systems, air-gapped or semi-isolated architectures minimize the impact of cyberattacks on physical operations.

Resilience engineering and Business Continuity Planning (BCP) are integral to the framework, ensuring rapid recovery during incidents. Redundancy, failover systems, and backup infrastructures support operational continuity even under attack conditions.

Finally, the human factor remains a critical component. Security awareness programs, role-based access control (RBAC), multi-factor authentication (MFA), and incident response training enhance organizational security maturity [6], [11].

In summary, the proposed framework provides a holistic, multi-layered security model that combines technical, organizational, and strategic measures. Its implementation can significantly enhance both the cybersecurity resilience and operational continuity of digital logistics systems operating within the East–West Transport Corridor.

Conclusion

This study has thoroughly examined the multifaceted and systemic nature of cybersecurity risks in digital logistics systems operating within the East–West Transport Corridor. While digitalization—through IoT integration, cloud infrastructures, real-time data flows, and automated management systems—enhances operational efficiency, it simultaneously broadens the attack surface and introduces more complex and unpredictable risk structures.

A key theoretical finding is that cybersecurity in digital logistics has evolved beyond a conventional "IT problem" and must be understood as a socio-technical and geo-economic risk. Cyber incidents in these systems can disrupt not only technological infrastructure but also supply chain stability and cross-border trade continuity.

Empirical analysis shows that, in highly integrated and multi-country systems like the East–West Corridor, risks arise not only from technological vulnerabilities but also from institutional and structural gaps. Heterogeneity in security standards, uneven maturity across vendor ecosystems, and differences in cross-border data governance create systemic weaknesses that can escalate local incidents into regional disruptions through cascading failures.

The study further highlights that modern cyber threats are non-linear, adaptive, and dynamic. Traditional perimeter-based security models are insufficient and must be complemented by adaptive paradigms such as Zero Trust Architecture, AI-driven anomaly detection, and real-time threat intelligence sharing. These approaches support both reactive defense and proactive risk mitigation.

The proposed integrated cybersecurity framework emphasizes that resilience in logistics systems depends on a combination of technical defenses, strengthened governance, regional cooperation, and harmonized supply chain security standards. This underscores the necessity of a multidisciplinary approach to cybersecurity management.

At the policy level, findings stress the importance of coordinated strategies among corridor countries. Without joint CERT mechanisms, real-time incident response platforms, and standardized compliance frameworks, ensuring long-term resilience of regional logistics networks remains highly challenging.

Future research should focus on three priority areas: (1) AI-based real-time risk prediction models, (2) transnational data governance and legal compliance mechanisms, and (3) resilience engineering approaches in cyber-physical logistics systems. Advancements in these domains will deepen theoretical and practical understanding of cybersecurity in logistics.

In conclusion, cybersecurity in digital logistics is not merely a technical concern but a complex, systemic risk encompassing economic, institutional, and geopolitical dimensions. The safe, efficient, and sustainable operation of the East–West Transport Corridor relies on the integrated, multi-layered, and coordinated management of these risks.

References

1. National Institute of Standards and Technology (NIST). Zero Trust Architecture. Gaithersburg: NIST. 800-207 (2020).
2. European Union Agency for Cybersecurity. Cybersecurity for Transport Sector. Athens: ENISA (2023).
3. Threat Landscape for Supply Chain Attacks. European Union Agency for Cybersecurity. ENISA (2021).
4. World Economic Forum. Global Cybersecurity Outlook 2024. Geneva: WEF (2024).
5. IBM Security. Cost of a Data Breach Report 2024. Armonk: IBM Corporation (2024).
6. Microsoft. Digital Defense Report 2023. Redmond: Microsoft Security (2023).
7. Cisco Systems. Cybersecurity Readiness Index 2023. San Jose: Cisco (2023).
8. Top Trends in Cybersecurity 2024. Stamford: Gartner Research (2024).
9. International Organization for Standardization (ISO). ISO/IEC 27001:2022 Information Security Management Systems — Requirements. Geneva: ISO (2022).
10. MITRE Corporation. MITRE ATT&CK Framework (Enterprise Version). Bedford: MITRE (2023).
11. Accenture. State of Cyber Resilience 2023. Dublin: Accenture Security (2023).
12. McKinsey & Company (2022). Cybersecurity in the Age of AI and Automation. New York: McKinsey Global Institute (2022).
13. Humayed, A., Lin, J., Li, F., Luo, B. Cyber-physical systems security: A survey update. IEEE Internet of Things Journal, 8(12), 9461–9482 (2021).
14. Sarker, I.H. AI-based cybersecurity: A modern review. Journal of Big Data, 8(1), 1–25 (2021).
15. Zhang, Y., Chen, J. IoT security in smart logistics systems. Sensors, 22(4), 1–21 (2022).
16. World Bank. Digital Logistics and Trade Corridors Report. Washington, DC: World Bank (2022).