European Research Studies Journal
Volume XXIX, Issue 1, 2026

pp. 527-538

The Impact of Logistical Disruptions on Enterprise Security Management – Implications for Energy Security

Submitted 13/12/25, 1st revision 15/01/26, 2nd revision 10/02/26, accepted 14/03/26

Tomasz Grudniewski[1], Zbigniew Ciekanowski[2], Marian Kopczewski[3], Sławomir Mazur[4], Jarosław Wołejszo[5], Krzysztof Drabik[6]

Abstract:

Purpose: *The aim of this article is to determine the impact of logistical disruptions on the process of enterprise security management and to identify factors that increase organisational resilience in conditions of supply chain instability. The issue addressed is the assessment of the importance of logistics security as an element of organisations' security management systems operating in a dynamic and uncertain economic environment.*
Design/Methodology/Approach: *The study used theoretical and empirical methods, including a literature review, systems analysis, and statistical analysis of transport, logistics, and supply chain disruptions. Data from international and national statistical institutions relating to the functioning of the logistics sector and the security of business operations were used. The research problem was formulated as follows: To what extent do logistics disruptions affect the security management system of enterprises and their ability to maintain business continuity? The research hypothesis posits that an increase in logistical disruptions significantly reduces business security, thereby necessitating the implementation of integrated logistical risk and business continuity management systems.*
Findings: *The analysis indicates that logistical disruptions are a significant risk factor affecting the operational, financial and organisational security of enterprises. An increase in the frequency of supply chain interruptions reduces the stability of an organisation's operations and forces the implementation of integrated logistics risk and business continuity management systems.*
Practical Implications: *The results of the study indicate the need to implement solutions that enhance the logistical security of enterprises, particularly through diversification of supply sources, the development of logistical risk-monitoring systems, the maintenance of safety*

[1]*John Paul II University in Biała Podlaska, Poland, ORCID: 0000-0003-3394-8992, e-mail: gisbourne2@gmail.com;*
[2]*War Studies University, Poland, ORCID 0000-0002-0549-894X, e-mail: zbigniew@ciekanowski.pl;*
[3]*Military University of Land Forces in Wrocław, Poland, ORCID: 0000-0002-0402-047, e-mail: marian.kopczewski@interia.pl;*
[4]*Andrzej Frycz Modrzewski University in Krakow, Poland, ORCID: 0000-0002-5056-2280, e-mail: smazur@orange.pl;*
[5]*President Stanisław Wojciechowski University of Kalisz, Poland, ORCID: 0000-0002-7216-3496, e-mail: j.wolejszo@uniwersytetkaliski.edu.pl;*
[6]*University of Siedlce, Poland, ORCID: 0000-0002-6555-1124 krzysztof.drabik@uws.edu.pl;*

stocks, and the implementation of business continuity and organisational resilience management procedures.

Originality/Value: *The article's value lies in presenting logistical disruptions as a key determinant of enterprise security management and in integrating logistics' perspective with the concepts of organisational security and enterprise resilience. The study points to the need to treat logistical security as a strategic element of modern organisations' security management systems.*

Keywords: *Logistics security, energy security, supply chain disruptions, enterprise security management, logistics risk, organisational resilience.*

JEL codes: *L92, F52, Q40, Q48, M21.*

Paper type: *Research article.*

1. Introduction

Dynamic changes in the modern economic environment mean that the security of business operations is becoming a key area of organisational management. Progressive globalisation, the development of international supply chains and the growing dependence of enterprises on complex logistics systems mean that logistics no longer performs an exclusively operational function, but has become a strategic element determining the stability and continuity of economic activity. As a result, disruptions to logistics processes affect not only the economic efficiency of enterprises, but also their organisational, operational and financial security.

In recent years, there has been a marked increase in factors destabilising the functioning of logistics systems, driven by geopolitical, technological, and socio-economic conditions. The COVID-19 pandemic, armed conflicts, energy crises, transport restrictions, cyber threats and instability in commodity markets have led to numerous disruptions in global and regional supply chains.

These phenomena have revealed companies' vulnerability to logistical disruptions and highlighted the need to implement new security management models based on risk analysis, organisational resilience, and business continuity. In this context, energy security is understood as the ability to ensure the continuity of energy and fuel supplies (at acceptable acquisition costs) necessary to maintain operational and logistical processes.

Logistics security is now an integral component of a company's security management system, covering the processes of planning, organising and controlling the flow of raw materials, information and products in a way that minimises risks

that could disrupt the organisation's objectives. Improper management of logistics can lead to serious consequences, such as production downtime, liquidity issues, decreased competitiveness, or a weakening of the company's market position. Thus, logistical disruptions should be seen as a significant risk factor affecting the level of security of an organisation's operations.

The issue addressed is part of the current trend in research on organisational resilience and security management in the context of growing economic uncertainty, underscoring the need to treat logistics as a fundamental pillar of security for modern enterprises.

2. Logistics Security as an Element of the Enterprise Security Management System

Contemporary enterprises operate in an environment characterised by high volatility and an increasing number of threats affecting the stability of operational processes (Ciekanowski *et al.,* 2024; Kadlubek *et al.,* 2022).

In these conditions, organisational security is no longer defined solely by the protection of material or information resources, but also by the enterprise's ability to maintain business continuity despite internal and external disruptions. One of the key components of this system is logistics security, which determines the efficient flow of raw materials, products and information throughout the supply chain (Christopher, 2023).

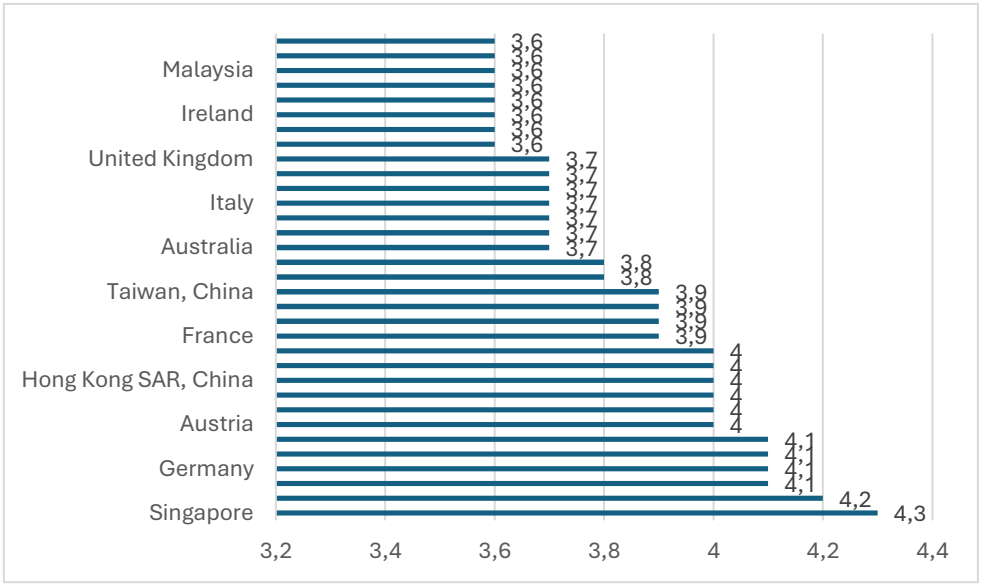
The development of global supply chains has increased companies' dependence on external entities, transport infrastructure, and IT systems supporting logistics processes (Żurawski *et al.,* 2025).

According to World Bank data, countries' logistical efficiency, measured by the Logistics Performance Index (LPI), remains one of the main factors determining companies' competitiveness and the security of their operations. In 2023, the average global delivery timeliness was around 3.2 on a five-point scale, indicating a continuing risk of transport delays and logistical disruptions that affect economic activity (World Bank, 2023). The data is presented in the chart below.

Logistics security can be defined as the ability of a company's logistics system to ensure the uninterrupted execution of procurement, production and distribution processes while limiting the risk of disruptions that could lead to operational or financial losses.

The literature on the subject emphasises that logistics is now a strategic area of organisational risk management, as even a short-term supply interruption can cause production stoppages and the loss of the ability to meet contractual obligations (Ivanov and Dolgui, 2020).

Figure 1. *Level of logistics efficiency of countries, measured by the Logistics Performance Index (LPI).*



Source: *World Bank, 2023.*

The importance of logistics security has increased particularly after the experience of the COVID-19 pandemic, when, according to OECD analyses, over 60% of manufacturing companies in OECD countries reported serious disruptions in their supply chains, leading to reduced production or temporary suspension of operations. This clearly indicates that logistical risk has become a dominant threat to enterprises' economic security (OECD, 2022).

In addition, Eurostat data indicate that freight transport costs in the European Union increased by more than 30% between 2020 and 2023, directly affecting the financial stability of companies and the level of operational risk in the manufacturing and trade sectors. The increase in logistics costs and the instability of transport flows necessitate the implementation of new security management models based on risk analysis and organisational resilience (Eurostat, 2024).

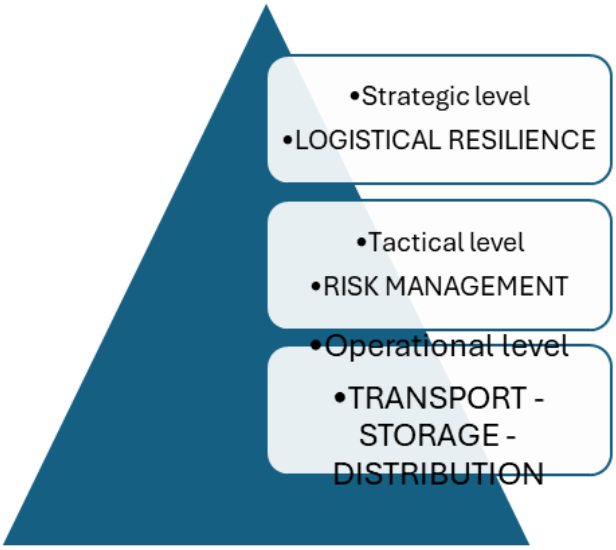
In the context of enterprise security management, logistics plays a critical role, and any disruption can trigger a domino effect that affects an organisation's production, financial, and reputational processes. For this reason, there are increasing calls for integrating logistics management with Business Continuity Management (BCM) and risk management systems compliant with ISO 22301 and ISO 31000 (Pettit, Fiksel, and Croxton, 2019). In practice, this integration should be supported by management control mechanisms that enable the monitoring of security objectives and the effectiveness of security measures (Chodyka *et al.,* 2025b).

Based on an analysis of the literature and statistical data, we can propose our own approach to logistics security as an integrated subsystem of enterprise security management, comprising three interrelated levels:

1. Operational level – continuity of transport, storage and distribution,
2. Tactical level – management of supplier and logistics infrastructure risk,
3. Strategic level – building the logistical resilience of the organisation (Logistic Security Resilience – LSR).

The above model is presented in Figure 2 below.

Figure 2. *Hierarchical Model of Enterprise Logistics Security.*



Source: *Own work.*

This model assumes that logistics security is not a separate function of the enterprise, but an element of systemic security management that affects the organisation's ability to adapt to economic and geopolitical crises. The integration of logistics processes with risk management enables the enterprise to limit the effects of disruptions and enhance the stability of its operations in conditions of environmental uncertainty. The presented approach is a starting point for further analysis of logistical disruptions as contemporary threats to enterprise security, which will be developed in the next part of the article.

4. Logistical Disruptions as a Contemporary Threat to the Functioning of Enterprises

The ongoing globalisation of the economy and the development of international production networks have significantly increased the complexity of supply chains, thereby increasing companies' vulnerability to logistical disruptions. Contemporary

logistics systems are characterised by a high level of interdependence among suppliers, transport operators, and end customers, meaning that even a local disruption can have global consequences. This phenomenon is referred to in the literature as the risk propagation effect in the supply chain (Tang, 2006).

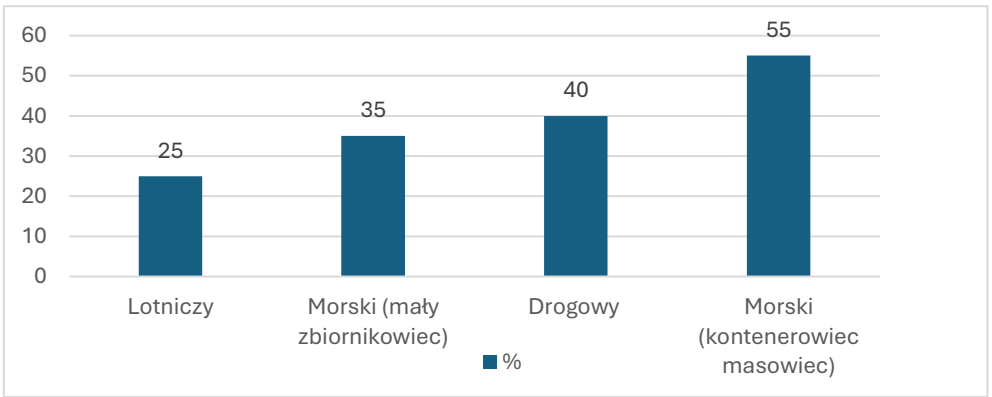
Logistical disruptions are events that cause a reduction or complete interruption in the flow of goods, services, or information within a company's logistics system. They can result from natural, economic, technological or political factors. Research shows that modern companies are increasingly experiencing multidimensional disruptions affecting transport, production and the availability of raw materials simultaneously (Ivanov, Dolgui, and Sokolov, 2019).

One of the key factors destabilising companies' operations was the impact of the COVID-19 pandemic, which led to unprecedented disruptions in global supply chains. According to analyses, over 70% of manufacturing companies worldwide reported logistical disruptions resulting in reduced operational capacity. At the same time, the pandemic revealed the excessive concentration of supply sources and the logistical inflexibility of many organisations, significantly affecting the security of their operations.

Geopolitical tensions and armed conflicts affecting the availability of transport infrastructure and the stability of raw material markets also remain a significant source of logistical risk. Companies operating in global logistics networks are particularly vulnerable to disruptions resulting from trade restrictions, economic sanctions and the destabilisation of transit regions.

The Russian-Ukrainian conflict has led, among other things, to restrictions on road and rail transport in Central and Eastern Europe and an increase in energy and fuel costs, which has directly translated into higher logistics costs for companies. The chart below shows the share of fuel in the costs of different modes of transport.

Figure 3. *Share of fuel in the costs of different modes of transport.*



Source: *European Commission.*

According to the analysis of the data presented, the share of fuel costs in road transport exceeds 40%, while in maritime container transport it exceeds 50%, making companies highly vulnerable to fluctuations in energy commodity prices. As a result, logistical disruptions in the fuel and energy carrier sector should be treated as a direct risk factor for companies' energy security.

Eurostat statistics confirm the scale of these changes, indicating an increase in freight transport costs in the European Union of over 30% between 2020 and 2023. At the same time, significant fluctuations in the volumes of road and sea transport have been recorded, indicating the growing instability of the logistics systems of companies operating on the European market (Eurostat, 2024).

The literature on the subject also emphasises the growing importance of technological and cyber threats to logistics security. The digitisation of transport processes and the use of warehouse and transport management systems (WMS, TMS) increase operational efficiency but also increase vulnerability to cyberattacks that can disrupt logistics flows. Cyber incidents can lead to the shutdown of logistics operations on a scale comparable to natural disasters (Ciekanowski *et al.,* 2024; Chodyka *et al.,* 2025a).

Another significant factor in logistical disruptions is the increase in energy costs and the limited availability of strategic raw materials. OECD reports indicate that between 2021 and 2023, over 60% of European companies experienced problems related to the availability of production components and longer delivery times, which forced them to reorganise their logistics strategies and increase their safety stock levels (OECD, 2023).

Logistical disruptions affect companies in a systemic way, leading to increased operational, financial and reputational risks. A lack of logistical resilience is one of the main reasons for organisations losing their ability to adapt in crisis situations.

As a result, companies are increasingly implementing resilience strategies, including supplier diversification, regionalisation of production, and the development of logistical risk-monitoring systems.

5. Adaptive Strategies for Managing Enterprise Security in Conditions of Logistical Instability

The increase in the frequency of logistical disruptions necessitates a redefinition of traditional enterprise security management models. Contemporary organisations are moving away from a reactive approach focused on eliminating the effects of disruptions, towards an adaptive approach aimed at building adaptive capacity and systemic resilience. In management literature, this process is referred to as a transformation towards resilient enterprise management (Hamel and Välikangas, 2003).

Logistical disruptions affect corporate decision-making primarily by increasing operational uncertainty and requiring strategic decisions in conditions of limited market predictability. Research by Wieland and Wallenburg (2013) indicates that companies with well-developed adaptive capabilities restore operational stability more quickly after supply chain disruptions.

An important element of security management in conditions of logistical instability is the integration of logistical processes with the company's strategic management. Effective reduction of logistical risk requires simultaneous management of supply flexibility, resource redundancy and supply chain visibility. Organisations implementing digital transport monitoring and predictive analytics systems demonstrate a higher level of operational security (Chopra and Sodhi, 2014).

Geographical diversification of suppliers and regionalisation of supply chains also play a significant role in increasing business security. Reports from the World Economic Forum indicate that, after 2020, more than 70% of multinational companies began shortening their supply chains (nearshoring) in response to growing logistical and geopolitical risks (World Economic Forum, 2023).

Adaptive logistics security management also includes developing organisational competencies in knowledge management and data analysis. The use of predictive analytics, artificial intelligence and decision support systems enables the early identification of potential logistics disruptions and limits their impact. The digital transformation of logistics significantly increases companies' resilience to disruptions in global goods flows (Dubey *et al.,* 2021).

The growing scale of logistical disruptions is forcing companies to redefine their approach to organisational security management. Contemporary enterprise security management focuses not only on minimising risk but, above all, on increasing the organisation's ability to operate in conditions of operational uncertainty and supply chain instability. The literature on the subject indicates that enterprise security is becoming directly linked to the level of logistical flexibility and the ability to quickly reconfigure supply processes (Ponomarov and Holcomb, 2009).

Logistical disruptions necessitate strategic decisions regarding the structure of supply, production location and transport organisation. Research by Scholten and Schilder (2015) indicates that companies with high levels of logistical integration and supplier partnerships are more resilient to operational disruptions. This means that business security should be built across the entire supply chain, not just within a single organisation.

One of the basic ways to strengthen business security is to diversify supply sources. Excessive concentration of suppliers increases companies' vulnerability to regional crises, transport restrictions, or political instability. Companies with alternative

supply channels reduce the time needed to return to full operational capacity by up to several dozen per cent after logistical disruptions (Simchi-Levi *et al.,* 2014).

The development of digital logistics management systems is also an important element in increasing organisational security. The implementation of real-time transport monitoring tools, data analytics systems, and supply chain management platforms enables earlier identification of threats and the implementation of preventive measures. Companies that use digital solutions achieve a higher level of operational stability amid global disruptions.

Another area for strengthening business security is strategic inventory management. The just-in-time logistics model, while cost-effective, has proven particularly vulnerable to disruptions in transport and production. As a result, many companies are now implementing hybrid strategies that combine operational efficiency with maintaining safety stocks (Brandon-Jones *et al.,* 2014).

The development of business continuity plans also plays a significant role in mitigating the effects of logistical disruptions. According to analyses by the International Organisation for Standardisation, implementing procedures compliant with ISO 22301 significantly reduces an organisation's response time to crisis situations and limits operational losses resulting from supply interruptions (ISO, 2019).

Based on the analyses carried out, key areas of action can be identified to increase the security of enterprises in the event of logistical disruptions:

1. Diversification of suppliers and transport routes, reducing dependence on individual logistics regions.
2. Development of supply chain monitoring systems that enable the ongoing identification of logistical threats.
3. Integration of logistics with enterprise risk management, including the incorporation of logistics processes into Enterprise Risk Management (ERM) systems.
4. Maintaining safety stocks for key production components.
5. Digitisation of logistics processes, including the use of data analytics and predictive systems.
6. Implementation of business continuity plans and contingency scenarios for transport and infrastructure disruptions.
7. Building partnerships in the supply chain to increase information exchange and coordination of crisis response.

Implementing these measures allows companies to reduce their vulnerability to logistical disruptions and increase the stability of their operations in a rapidly changing economic environment.

6. Conclusion

The analysis shows that modern organisations operate in an increasingly unstable economic environment, in which logistics is becoming a key determinant of operational security. The globalisation of economic processes, the development of complex supply chains, and the ongoing digitisation of logistics have increased companies' operational efficiency but also heightened their vulnerability to transport, economic, geopolitical, and technological disruptions.

The first part of the article shows that logistics security is an integral part of a company's security management system, determining the continuity of supply, production and distribution processes. The efficient functioning of logistics systems directly impacts an organisation's operational stability, and their disruption can lead to serious financial and organisational consequences. Logistics is therefore no longer merely a support function for a company's operations, but has become a strategic pillar of its security.

The second part of the study confirmed that logistical disruptions are currently among the most significant threats to the functioning of enterprises. An analysis of literature and statistical data indicated the significant impact of the COVID-19 pandemic, rising energy and fuel prices, geopolitical tensions, and infrastructure constraints on the stability of global and regional supply chains. These phenomena generate a cascading effect, transferring the effects of disruptions between successive links in the logistics system, which in turn increases operational and financial risk for enterprises.

The third part of the article points out that effective management of enterprise security in conditions of logistical instability requires the implementation of adaptive management strategies to increase organisational resilience. Of particular importance are measures such as supplier diversification, the development of digital supply chain monitoring systems, the integration of logistics with enterprise risk management processes, and the implementation of business continuity plans. Companies that can flexibly reconfigure their logistics processes demonstrate higher operational security and greater adaptability in crisis situations.

The results obtained allow us to conclude that logistical disruptions should not be treated solely as an operational problem, but as a strategic management challenge affecting the long-term stability of companies. The security of an organisation increasingly depends on its ability to anticipate logistical threats, respond quickly to environmental changes, and build flexible, resilient supply chain structures.

The analyses indicate that modern companies should develop an integrated approach to security management, including logistics as a key strategic area. It is necessary to move away from the cost-optimisation model in favour of balancing economic efficiency with operational security. In practice, this means investing in digital

technologies, developing supply chain partnerships, maintaining operational reserves, and systematically improving crisis response procedures.

In summary, logistics security is currently one of the fundamental conditions for the stable functioning of enterprises in the global economy. Organisations that effectively manage logistics risk and implement solutions to increase operational resilience achieve higher levels of security, competitiveness and long-term sustainability.

References:

Brandon-Jones, E., Squire, B., Autry, C.W., Petersen, K.J. 2014. A Contingent Resource-Based Perspective of Supply Chain Resilience and Robustness. Journal of Supply Chain Management, 50, 55-73.

Chodyka, M., Ciekanowski, Z., Kuznetsov, V., Żurawski, S., Chrząszcz, A.E., Drapikowska B. 2025a. The Role of Human Resource Management in Building an Organisational Security System, Including Cybersecurity, in the Era of Globalisation. European Research Studies Journal, Volume XXVIII, Issue 4, 1458-1470.

Chodyka, M., Nowicka, J., Mazur, S., Ciekanowski, Z., Król, A., Zdunek, M. 2025b. The Role of Management Control in Ensuring Organisational Security. European Research Studies Journal, Volume XXVIII, Issue 3, 03-14.

Ciekanowski, Z., Gruchelski, M., Nowicka, J., Zdunek, M., Zurawski, S. 2024. Risk Management and Organisational Resistance to Threats. European Research Studies Journal, Volume XXVII, Issue 1, 142-153.

Ciekanowski, Z., Nowicka, J., Czternastek, M., Zurawski, S., Mikosik, P. 2024. How Cybersecurity Shapes Effective Organisational Management. European Research Studies Journal, Volume XXVII, Issue 2, 454-464.

Christopher, M. 2023. Logistics and Supply Chain Management. Financial Times Prent.

Chopra, S., Sodhi, M. 2014. Managing Risk to Avoid Supply-Chain Breakdown. MIT Sloan Management Review, vol. 46, no. 1, 52-61.

Consilium. https://www.consilium.europa.eu/pl/.

Dubey, R., Bryde, D.J., Blome, C., Roubaud, D., Giannakis, M. 2021. Facilitating artificial intelligence powered supply chain analytics through alliance management during the pandemic crises in the B2B context. Industrial Marketing Management, Volume 96, 135-146.

Eurostat. https://ec.europa.eu/eurostat/web/transport/data/database.

Hamel, G., Välikangas, L. 2003. The Quest for Resilience. Harvard Business Review, 81, 52-63.

ISO - International Organisation for Standardisation. https://www.iso.org/home.html.

Ivanov, D., Dolgui, A. 2020. Viability of Intertwined Supply Networks: Extending the Supply Chain Resilience Angles towards Survivability. A Position Paper Motivated by COVID-19 Outbreak. International Journal of Production Research, 58, 2904-2915.

Ivanov, D., Dolgui, A., Sokolov, B. 2019. Ripple Effect in Supply Chains: Definitions, Frameworks and Future Research Perspectives. In: Handbook of Ripple Effects in the Supply Chain, Springer.

Kadłubek, M., Thalassinos, E., Noja, G.G., Cristea, M. 2022. Logistics customer service and sustainability-focused freight transport practices of enterprises: Joint influence of

organizational competencies and competitiveness. J. Green Econ. Low-Carbon Dev, 1(1), 2-15.

Pettit, T., Fiksel, J., Croxton, K. 2010. Ensuring Supply Chain Resilience: Development of a Conceptual Framework. Journal of Business Logistics, 31(1), 1-21.

Ponomarov, S., Holcomb, M. 2009. Understanding Supply Chain Resilience. The International Journal of Logistics Management, 20(1), 124-143.

Scholten, K., Schilder, S. 2015. The role of collaboration in supply chain resilience. Supply Chain Management: An International Journal, 20(4), 471-484.

Simchi-Levi, D., Schmidt, W., Wei, Y. 2014. From superstorms to factory fires, managing unpredictable supply-chain disruption. Harvard Business Review, 92(1-2), 96.

Tang, S.C. 2006. Perspectives in supply chain risk management. International Journal of Production Economics, Volume 103, Issue 2, 451-488.

The Organisation for Economic Co-operation and Development, OECD. https://www.oecd.org/en.html.

World Bank. 2023. https://lpi.worldbank.org/.

Wieland, A., Wallenburg, C. 2013. The influence of relational competencies on supply chain resilience. International Journal of Physical Distribution & Logistics Management, 43(4), 300-320.

Zurawski, S., Ciekanowski, Z., Pauliuchuk, Y., Ratter, E. 2025. The Impact of Supply Chain Security Management on the Functioning of Modern Organisations. European Research Studies Journal, Volume XXVIII, Issue 1, 44-56.