ISSN: 2450-6869

eISSN: 2719-6763

No. 22, 2025

DEFENCE SCIENCE REVIEW

http://www.journalssystem.com/pno/

DOI: 10.37055/pno/220752

State Security and Supply Chains under Non-Kinetic Pressure

Original article

Received: 2026-02-22

Peer review:2026-02-25

Revised: 2026-03-30

Final review: 2026-03-31

Accepted: 2026-04-18

Double blind

Keywords:

state security, supply chain vulnerability, non-kinetic influence, cascading effects.

Krzysztof Kaczmarek[1,2,A-F]

ORCID 0000-0001-8519-1667

A - Research concept and design, B - Collection and/or assembly of data, C - Data analysis and interpretation, D - Writing the article, E - Critical revision of the article, F - Final approval of the article

[1]Politechnika Koszalińska, Poland

[2]Wydział Humanistyczny, Politechnika Koszalińska, Poland

Abstract

Objectives: The objective of the article is to analyse supply chains as an element of state security under conditions of non-kinetic influence. Particular attention is given to mechanisms of interference within supply chains and their consequences for the state's capacity to respond, taking into account structural complexity, multi-stage organisation, and the limited detectability of such actions.

Results: The results indicate that the vulnerability of supply chains is structural in nature and derives from their complexity, the dispersion of responsibility, and the selective and probabilistic character of control mechanisms. The analysis demonstrates that interference can be effectively embedded in routine and legally functioning economic processes, including the digital and informational layer, which facilitates the accumulation of effects and the emergence of cascading impacts at later stages of supply chain operation.

Conclusions: The article confirms that disruptions to supply chains may be employed as a tool of long-term, non-kinetic influence on the state, leading to a gradual weakening of institutional response capacities. From the perspective of state security, this necessitates treating supply chains as a permanent space of vulnerability, requiring an analytical approach that goes beyond logistics and procedural compliance.

Corresponding author Krzysztof Kaczmarek Politechnika Koszalińska, Poland; email: puola1972@gmail.com

1. Introduction

In the contemporary strategic environment, the security of states and societies increasingly depends on the stability and predictability of supply flows of raw materials and goods. This applies both to periods of relative stability and to situations of crisis. At the same time, ongoing digitalisation, economic interdependence, and the fragmentation of decision-making processes have made supply chains one of the key components of state security.

Modern supply chains should no longer be understood merely as an economic backbone. They constitute complex techno-organisational systems, embedded in production processes, transport infrastructure, information and communication technologies, regulatory frameworks, and human resources. In the sphere of production, this also includes the availability of inputs of appropriate quality, components, and critical raw materials. At the same time, the functioning of supply chains has become increasingly dependent on digital management systems, cross-border data flows, and close interaction between public and private actors. While such arrangements enhance efficiency, they simultaneously generate new vulnerabilities to disruption.

In recent years, there has been a growing relevance of activities commonly described as hybrid, conducted below the threshold of open armed conflict. These activities include cyber operations, information and disinformation campaigns, psychological influence, regulatory pressure, and limited acts of sabotage. Their primary objective is not the direct destruction of state systems, but the gradual erosion of institutional capacity, the increase of operational costs, and the weakening of public trust in the state as a provider of security. Within this context, supply chains represent a particularly attractive target. Their structural complexity, dispersed responsibility, and reliance on a stable information environment mean that even minor disturbances can produce cascading effects. Actions undertaken in one domain—such as the digital or informational domain—may generate consequences in the physical, social, and political spheres without the use of military force.

An important dimension of such influence is the perceptual sphere. The deliberate generation of uncertainty, a persistent sense of threat, and narratives undermining the state's ability to ensure continuity of supply may contribute to the normalisation of disruptions as a new baseline condition. Over time, this weakens societal resilience and reduces the capacity of the state to mobilise resources in response to crisis situations.

The aim of this article is to analyse supply chain security as an element of state security under conditions of non-kinetic pressure exerted by hostile external actors. The article focuses on identifying mechanisms of destabilisation in the digital, informational, psychological, and sabotage-related domains, as well as on assessing their impact on the functioning of logistical and institutional systems. In the subsequent sections, case studies are presented to illustrate these mechanisms in specific national contexts, allowing for the identification of patterns that are context-specific as well as those of a more universal character.

The article advances the hypothesis that disruptions to supply chains increasingly constitute a deliberately employed instrument of non-kinetic conflict, aimed at the long-term weakening of state capacity through multi-domain and cascading effects rather than through direct physical destruction.

To address this hypothesis, the study adopts a qualitative analytical approach grounded in polemological theory and employs case study analysis to examine supply chains as a contested space of contemporary interstate rivalry.

The contribution of the article lies in reinterpreting supply chain security not as a primarily logistical or economic challenge, but as an integral component of state security shaped by conflict dynamics below the threshold of armed warfare.

2. Methods

The study adopts a qualitative and analytical research design. Its objective is not to provide an empirical evaluation of the effectiveness of specific public policies, nor to conduct a normative analysis of strategic documents, but to identify and interpret mechanisms of conflict-related influence that affect supply chain security as a component of state security. The research perspective draws on a polemological approach, focusing on the study of conflict, its forms, dynamics, and instruments of influence under conditions other than classical armed warfare.

The analysis is grounded in the assumption that contemporary interstate conflicts increasingly take the form of prolonged pressure exerted below the threshold of open military force. From this perspective, disruptions to supply chains are not treated as unintended side effects of crises or instability, but as deliberately employed instruments of influence aimed at the gradual erosion of a state's capacity to function and respond effectively.

The polemological framework applied in this study enables the analysis of supply chains as a contested space of conflict, in which non-kinetic activities – such as cyber operations, information and psychological influence, economic pressure, and limited acts of sabotage – serve as tools of strategic competition. The analysis focuses on the interdependencies between different domains of influence and on the cascading effects they generate within the state security system.

In the empirical part of the article, a case study approach is employed. This method allows for an in-depth examination of conflict mechanisms within a specific national context, without pursuing statistical generalisation. The case study is used to identify patterns of influence, modes of adaptation to local conditions, and the limits of effectiveness of non-kinetic pressure.

The case analysis is based on the triangulation of factual materials, including secondary data derived from expert analyses, academic research, and verified media reporting. The use of triangulation is intended to enhance the credibility of interpretations and to reduce the risk of oversimplification of the phenomena under examination.

The analysis is conducted from the perspective of state security, based on the assumption that supply chains constitute an integral component of both a state's conflict potential and its strategic resilience. The adopted methodology makes it possible to capture

the conflictual nature of non-kinetic activities and their significance in processes of long-term destabilisation characteristic of contemporary forms of interstate competition.

3. Results

Supply chains are vulnerable to hostile actions at every stage and across all sectors, and this vulnerability has a systemic character. Risk emerges already at the stage of sourcing raw materials and components and subsequently accumulates across successive phases, including production, processing, storage, transportation, distribution, and the use of final products by end users.

The mechanism whereby interference introduced at an early stage of the supply chain – specifically at the level of raw material sourcing-produces effects that become visible only during final use is illustrated by the 2008 incident identified in the United States involving the deliberate contamination or falsification of heparin manufactured in China and used in pharmaceutical production. This incident resulted in numerous severe clinical reactions. Contaminated heparin was also detected in at least ten other countries, leading to regulatory responses at the international level (FDA, 2013).

Another example of interference with products within supply chains is provided by a series of incidents in Australia in 2018, when needles and metal objects were found in strawberries across the country. These acts of sabotage led to the destruction of crops and the loss of a significant number of jobs throughout the supply chain (The Guardian, 2018). The analytical findings are further corroborated by the case of falsified components for Boeing 787 aircraft, which passed quality control procedures despite material non-compliance (Landini, Hepher, 2025).

At the same time, analyses of threats related to supply chain interference at different stages indicate that such actions may be carried out at any point by individuals with authorised access to systems, making them particularly difficult to detect. As a result, the consequences of such interference often become apparent only at later stages of operation, despite the existence of control procedures (Kont et al., 2015, pp. 12-13).

The accumulated findings further indicate that interference in supply chains is not based on isolated, singular actions, but rather on the exploitation of structural features inherent to complex supply systems. The fragmentation of responsibility, outsourcing, and the involvement of multiple public and private actors create conditions in which accountability is dispersed and the detection of hostile activities is delayed or remains incomplete. Under such conditions, disruptions may be interpreted as technical failures, market fluctuations, or operational inefficiencies rather than as manifestations of deliberate interference (Tang, 2006, pp. 452-455).

The analysis also demonstrates that control mechanisms operating within supply chains primarily function as tools of risk reduction rather than as means of its complete elimination (Das, Perona, 2025, pp. 16-17; Emrouznejad, Abbasi, Sıcakyüz, 2023, p. 16). Quality assurance procedures, audits, and border controls are selective and probabilistic in nature, constrained by available resources, time pressure, and the high volume of legitimate flows (Karklina-Admine, et al., 2024, p. 11**)**. As a consequence, a structural margin of undetectability persists, enabling

manipulated, contaminated, or otherwise compromised products to enter and circulate within legal trade streams.

Empirical findings also confirm that the effects of disruptions are often cumulative. Small disruptions introduced intentionally or accidentally at upstream or intermediate links of the supply chain, which individually do not trigger alarm mechanisms, can reinforce one another at subsequent stages. This leads to cascading effects, including operational disruptions, increased costs, erosion of public trust, and reduced institutional capacity to respond effectively, particularly in crisis situations (Namdar, et al., 2024, p. 20).

In summary, the results indicate that supply chains constitute a space of vulnerability in contemporary national security systems. This vulnerability is not limited to periods of overt crisis but also manifests under conditions of apparent normality, when hostile actions can be woven into routine economic and logistical processes. This makes supply chains particularly vulnerable to prolonged, non-kinetic forms of pressure aimed at weakening a state's resilience.

In parallel with material and procedural forms of interference, the analysed cases also reveal a digital and informational dimension of influence on supply chains. In practice, such interference does not necessarily involve a direct attack on information technology infrastructure, but rather the exploitation of legitimate management systems, quality documentation, and digital mechanisms used to track product origin. Institutional reports indicate that attacks on supply chains increasingly take the form of introducing alterations or ambiguities into documentation, certificates, test reports, and compliance-related data, which enables modified or defective components to continue functioning within lawful economic circulation (ENISA, 2021, pp. 7-9).

In this context, a significant role is played by digital identification and traceability, which in complex, multi-stage supply chains is based on distributed data sets created and updated by multiple actors. From an empirical perspective, this means that supply chain integrity depends not only on the physical inspection of components, but also on the coherence and reliability of informational artefacts such as certificates, audit results, and compliance reports. As technical studies indicate, under real economic conditions full verification of such data is difficult, and inconsistencies may persist for extended periods without their authenticity being explicitly challenged (Pease, et al., 2024, pp. 12-15).

Empirical observations also confirm that the informational layer performs a reinforcing and masking function with regard to interference in supply chains. Delays in information flows, ambiguous communication following incidents, and fragmented access to data contribute to the dispersion of responsibility and hinder the rapid activation of corrective procedures. As a result, interference embedded in routine digital and informational processes may remain undetected at early stages, even when their material effects become apparent only at later levels of supply chain operation (ENISA, 2023, pp. 28-31).

4. Discussion

The presented results confirm that the vulnerability of supply chains to hostile, intentional actions stems from their structural complexity and multi-stage nature. This is consistent with previous research (Ivanov, Dolgui, 2021, p. 14; Dolgui, Ivanov, 2021, pp. 106-107; Monostori, 2021, p. 380; Li, Zobel, 2020, pp. 1-2). Earlier studies also emphasise that the level of cybersecurity has a direct impact on the vulnerability of supply chains to threats (Dash, et al., 2024, p. 13). At the same time, the results of the analysis indicate that interference in supply chains can be effectively embedded in and concealed within routine economic processes (Sodhi, et al., 2025, p. 234; Anzoom, Nagi, Vogiatzis, 2021). As a result, such actions are difficult to detect (Ashraf, Eltawil, Ali, 2024, p. 23).

One of the key conclusions is that risk does not concern a single point in the supply chain that is potentially most exposed to disruptions, but rather accumulates as it passes through successive stages (Ghadge, Ivanov, Chaudhuri, 2022, p. 6715). Consequently, even minor quality-related or procedural deviations introduced at early stages may generate effects that become noticeable only at the level of end use (Muralidharan, Hora, Bapuji, 2022, pp. 956-960).

Hostile, intentional interference in supply chains may be sufficiently discreet to be detected only when there is prior awareness of the possibility of such an incident or purely by chance. However, when such interference is embedded in legal and routine economic processes, its detection requires specialised procedures and analytical tools. This means that an approach based on identifying individual weak links is insufficient from the perspective of state security.

The results of the analyses also indicate that control mechanisms operating within supply chains are selective and probabilistic in nature. This, too, is confirmed by earlier studies (Wang, 2025, p. 1). At the same time, limited resources and time pressure make comprehensive control of all elements of the supply chain impossible. As a consequence, a structural margin of undetectability persists, which may be exploited to introduce interference that remains undetected at the point of entry.

An important finding of the analysis is the cumulative nature of the effects of interference in supply chains. Disruptions that individually do not trigger alarm mechanisms and are not identified as significant threats may reinforce one another as they move through successive stages of the supply chain. Over time, this leads to cascading effects, including operational disruptions, increased operating costs, and a gradual decline in institutional capacity to respond (Qazi, 2025, pp. 4-5).

From the perspective of state security, this necessitates viewing supply chains as a permanent space of vulnerability rather than merely an area of logistical risk. Their exposure is not limited to crisis situations but also manifests during periods of apparent stability, when interference may remain invisible or be interpreted as natural disruptions of economic processes. This makes supply chains particularly susceptible to long-term, non-kinetic forms of influence, the aim of which is not immediate destabilisation but the gradual

weakening of the system's capacity to adapt and respond (Lehdonvirta, Wú, Hawkins, 2025, pp. 1450-1455).

The obtained results therefore suggest the need to move away from perceiving supply chain security solely in terms of control and procedural compliance. Instead, an analytical approach is required that takes into account the limitations of detectability and the inevitable nature of residual risk resulting from the selectivity of control mechanisms and the complexity of contemporary supply systems.

The presented findings support the hypothesis adopted in the article, according to which supply chain disruptions do not constitute incidental disturbances of logistical processes, but rather a deliberately employed instrument of long-term non-kinetic influence, leading to the gradual weakening of the state's capacity to respond.

An additional problem is the limited possibility of unequivocal attribution of such interference which, embedded in normal market and operational fluctuations, is often not identified as hostile action but interpreted as technical failures, organisational errors, or the consequences of economic pressure. This mechanism manifests itself with particular intensity in long, transnational, and highly digitalised supply chains, in which responsibility is dispersed among multiple public and private actors and decision-making processes are fragmented (Prasad, et al., 2025, pp. 5-7).

At the same time, it should be emphasised that the conducted analysis is based on available empirical cases and secondary sources, which limits the possibility of fully reconstructing all mechanisms of interference. These limitations do not, however, undermine the system-level conclusions, but instead point to the need for further in-depth research, particularly in the area of identifying subtle and long-term forms of influence.

In light of the presented findings, supply chains emerge as one of the key areas of vulnerability in contemporary state security systems. Their analysis requires a perspective that goes beyond logistics and economics, encompassing also the strategic and security dimensions appropriate for assessing threats of a non-kinetic, long-term, discreet nature, oriented towards weakening state security.

5. Conclusions

The results of the conducted analysis show that supply chains constitute one of the key areas of vulnerability in contemporary state security systems. Their susceptibility does not stem solely from individual weak points or incidental disruptions, but from the very structure of modern supply systems, which are characterised by multi-stage organisation, complexity, and the dispersion of responsibility. Under such conditions, even seemingly marginal forms of interference may accumulate over time and across stages, leading to cascading effects whose consequences become apparent only at later phases of the supply chain's operation.

The findings of the article confirm the hypothesis that supply chain disruptions can be employed as an instrument of long-term, non-kinetic influence on the state. Such actions, embedded in routine and legally operating economic processes, often remain difficult to detect, while their identification is further constrained by the selective and probabilistic nature

of control mechanisms. As a result, a structural margin of undetectability persists, facilitating the gradual weakening of institutional response capacities without triggering unambiguous crisis signals. The obtained findings indicate that supply chain security cannot be analysed exclusively in terms of procedural compliance or logistical efficiency. Instead, it requires a systemic approach that takes into account the enduring nature of vulnerability, the limitations of detectability, and the inevitable existence of residual risk. Particular attention should therefore be paid to supply chains, especially in the context of the current tense international environment.

From the perspective of state security, this implies the necessity of treating supply chains as a permanent component of the threat environment, in which influence is dispersed, long-term, and difficult to attribute unequivocally. At the same time, the results of the article point to the need for further in-depth research focused on identifying subtle forms of interference and the mechanisms through which they accumulate over time.

References

Anzoom, R., Nagi, R., & Vogiatzis, C. (2021). A review of research in illicit supply-chain networks and new directions to thwart them. *IISE Transactions, 54*(2), 134–158. https://doi.org/10.1080/24725854.2021.1939466

Ashraf, M., Eltawil, A., & Ali, I. (2024). Disruption detection for a cognitive digital supply chain twin using hybrid deep learning. *Operational Research, 24*(2), 23. https://doi.org/10.1007/s12351-024-00831-y

Das, S. K., & Perona, M. (2025). Supply chain risk management automation: A literature review. *Electronic Markets, 35*, 104. https://doi.org/10.1007/s12525-025-00844-1

Dash, A., Sarmah, S. P., Tiwari, M. K., Jena, S. K., & Glock, C. H. (2024). Cybersecurity investments in supply chains with two-stage risk propagation. *Computers & Industrial Engineering, 197*, 110519. https://doi.org/10.1016/j.cie.2024.110519

Dolgui, A., & Ivanov, D. (2021). Ripple effect and supply chain disruption management: New trends and research directions. *International Journal of Production Research, 59*(1), 102–109. https://doi.org/10.1080/00207543.2021.1840148

Emrouznejad, A., Abbasi, S., & Sıcakyüz, Ç. (2023). Supply chain risk management: A content analysis-based review of existing and emerging topics. *Supply Chain Analytics, 3*, 100031. https://doi.org/10.1016/j.sca.2023.100031

Ghadge, A., Er, M., Ivanov, D., & Chaudhuri, A. (2022). Visualisation of ripple effect in supply chains under long-term, simultaneous disruptions: A system dynamics approach. *International Journal of Production Research, 60*(20), 6173–6186. https://doi.org/10.1080/00207543.2021.1987547

Ivanov, D., & Dolgui, A. (2021). OR-methods for coping with the ripple effect in supply chains during COVID-19 pandemic. *International Journal of Production Economics, 232*, 107921. https://doi.org/10.1016/j.ijpe.2020.107921

Karklina-Admine, S., Cevers, A., Kovalenko, A., & Auzins, A. (2024). Challenges for customs risk management today: A literature review. *Journal of Risk and Financial Management, 17*(8), 321. https://doi.org/10.3390/jrfm17080321

Lehdonvirta, V., Wú, B., & Hawkins, Z. (2025). Weaponised interdependence in a bipolar world. *Review of International Political Economy, 32*(5), 1442–1467. https://doi.org/10.1080/09692290.2025.2489077

Li, Y., & Zobel, C. W. (2020). Exploring supply chain network resilience in the presence of the ripple effect. *International Journal of Production Economics, 228*, 107693. https://doi.org/10.1016/j.ijpe.2020.107693

Monostori, J. (2021). Mitigation of the ripple effect in supply chains. *CIRP Journal of Manufacturing Science and Technology, 32*, 370–381. https://doi.org/10.1016/j.cirpj.2021.01.013

Muralidharan, E., Hora, M., & Bapuji, H. (2022). Hazard severity and time to recall. *Journal of Business Research, 139*, 954–963. https://doi.org/10.1016/j.jbusres.2021.10.035

Namdar, J., Blackhurst, J., Zhao, K., & Song, S. (2024). Cascading disruptions: Impact of modularity and nexus supplier predictions. *Journal of Supply Chain Management, 60*(3), 18–38. https://doi.org/10.1111/jscm.12326

Prasad, N., Diro, A., Warren, M., & Fernando, M. (2025). A survey of cyber threat attribution. *Computers & Security, 157*, 104606. https://doi.org/10.1016/j.cose.2025.104606

Qazi, A. (2025). Systemically important supply chains in crisis. *Natural Hazards Research*. https://doi.org/10.1016/j.nhres.2025.09.003

Sodhi, M. S., Roscoe, S., Ellram, L. M., Tang, C., Sarkis, J., Handfield, R. B., Roehrich, J. K., & Schleper, M. C. (2025). Infiltration, interdiction, and other covert supply chain operations. *International Journal of Operations & Production Management, 45*(13), 233–252. https://doi.org/10.1108/IJOPM-02-2025-0115

Tang, C. S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics, 103*(2), 451–488. https://doi.org/10.1016/j.ijpe.2005.12.006

Wang, T. C. (2025). Development of a cost-effective inspection scheme. *International Journal of Production Economics, 288*, 109714. https://doi.org/10.1016/j.ijpe.2025.109714

Other sources

ENISA. (2021). *ENISA threat landscape for supply chain attacks*. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%20for%20Supply%20Chain%20Attacks.pdf

ENISA. (2023). *ENISA threat landscape 2023*. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

FDA. (2013). *Guidance for industry: Heparin for drug and medical device use*. https://www.fda.gov/files/drugs/published/Heparin-for-Drug-and-Medical-Device-Use---Monitoring-Crude-Heparin-for-Quality.pdf

Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., & Osula, A. M. (2015). *Insider threat detection study*. NATO CCDCOE. https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf

Landini, F., & Hepher, T. (2025, March 13). Insight: How faulty parts on Boeing's 787 jets flew below the radar in Italy. *Reuters*. https://www.reuters.com/business/aerospace-defense/how-faulty-parts-boeings-787-jets-flew-below-radar-italy-2025-03-13/

Pease, M., Wallace, E., Reed, H., Martin, V. L., & Granata, S. (2024). *Supply chain traceability: Manufacturing meta-framework (NIST IR 8536)*. NIST. https://doi.org/10.6028/NIST.IR.8536.ipd

The Guardian. (2018, September 17). *Strawberry needle sabotage scare spreads to all six Australian states*. https://www.theguardian.com/australia-news/2018/sep/17/australian-police-say-needle-found-in-banana-as-strawberry-sabotage-spreads