LORE
19,1

32

Received 28 April 2025
Revised 11 June 2025
17 October 2025
Accepted 25 November 2025

Systematic node fortification for enhanced supply network resilience: a real-world network approach

Patrick Doege and Kai-Oliver Schocke
Frankfurt University of Applied Sciences, Frankfurt am Main, Germany, and
Maike Scherrer
School of Engineering, Zurich University of Applied Sciences, Zurich, Switzerland

Abstract

Purpose – This study questions the need for more visibility to improve supply chain network resilience (SCNR). It investigates how disruptions propagate through real-world supply chain networks and evaluates the effectiveness of different strategies for fortifying key nodes against such disruptions. The aim is to identify practical, data-driven methods that enhance SCNR by prioritising critical nodes for protection using social network analysis (SNA) metrics.
Design/methodology/approach – Agent-based modelling combined with the susceptible–infected–recovered (SIR) model from epidemiology literature is applied to simulate disruption propagation in ten real-world supply chain networks. Fortification strategies are based on five SNA metrics and evaluated against random node selection. Fortification is implemented by increasing a node's resistance to disruption and accelerating its recovery, an abstract representation of real-world resilience measures such as redundancy, information sharing or collaborative strategies. Each scenario is tested under single-node and multi-node disruption conditions, with 100 repetitions per configuration to ensure robustness.
Findings – Targeted node fortification based on SNA metrics significantly outperforms random fortification in reducing performance loss. While page rank yields best resilience benefits on average, simpler metrics like node degree deliver nearly equivalent improvements, demonstrating that effective resilience strategies can be implemented without requiring full network visibility.
Originality/value – This research closes a relevant gap in SCNR literature by validating fortification strategies on realistic, large-scale supply chain networks, moving beyond idealised or synthetic structures. Findings provide actionable, scalable guidance for supply chain practitioners, demonstrating that even basic network metrics enable meaningful resilience improvements in complex supply chains.

Keywords Supply chain network resilience, Disruption propagation, Node fortification strategies, Social network analysis in supply chains, Agent-based simulation

Paper type Research article

1. Introduction

Supply chain network resilience (SCNR) has become an important topic in recent literature, focusing on the ability of supply networks to withstand and recover from disruptions (Chopra and Sodhi, 2004; Ivanov, 2018). With increasing complexity of global supply networks, disruptions caused by pandemics, natural disasters and geopolitical events (Li and Zobel, 2020) lead to widespread material shortages and operational shutdowns across networks. These interconnected systems often experience cascading disruptions, known as the ripple effect (Ivanov *et al*., 2014), highlighting the difficulty of predicting, managing and containing such risks (Li and Zobel, 2020). Despite the increasing focus on SCNR, there is still a gap in understanding how disruptions propagate through these complex networks (Basole and Bellamy, 2014) and eventually dissipate (Habibi *et al*., 2025), with limited practical guidance for supply chain management (SCM) practitioners.

Logistics Research
Vol. 19 No. 1, 2026
pp. 32-46
Emerald Publishing Limited
e-ISSN: 1865-0368
p-ISSN: 1865-035X
DOI 10.1108/LORE-04-2025-0050

This paper forms part of a special section "Digital Transformation in Transport and Logistics", guest edited by Dr Ralf Elbert and Dr Hongjun Wu.

However, current research on SCNR dynamics primarily assumes homogeneous risk capabilities across nodes (Li *et al*., 2021) and focuses on idealised network structures (Li and Zobel, 2020), overlooking the practical challenges faced by SCM practitioners. Proposed approaches to increase SCNR, such as restructuring entire networks, are often unrealistic in practice (Basole and Bellamy, 2014; Zhao *et al*., 2011). Furthermore, while increasing node risk capacity is more effective than adjusting network structure (Li and Zobel, 2020), it is impractical to strengthen all nodes (Li and Zobel, 2020) due to the significant costs and resource requirements involved. This highlights an important theoretical gap: Identifying which subset of critical nodes should be prioritised for fortification, to efficiently enhance SCNR, remains an unresolved challenge.

The purpose of this paper is to address this gap by investigating how disruptions propagate through real supply chain networks, how a fortification of key nodes against disruptions affects this propagation and which selection strategy for node fortification is most effective. Building on previous work of Doege and Scherrer (2022), we extend the simulation experiments by using a dataset published in the Manufacturing & Service Operations Management (MSOM) journal (Willems, 2007), which includes real supply chain networks from different industries. This allows to validate previous findings with realistic data and provide practical insights for SCM practitioners. Our approach offers a novel strategy for improving SCNR by focusing on targeted node fortification, and thus contributes to the ongoing discussion on SCNR both theoretically and practically.

2. Literature review

The term "supply chain resilience" originated in the early 2000s (Rice and Caniato, 2003; Christopher and Peck, 2004) and generally refers to a supply chain's "adaptive capability [. . .] to prepare for unexpected events, respond to disruptions, and recover from them by maintaining continuity of operations at the desired level of connectedness and control over structure and function" (Ponomarov and Holcomb, 2009, p. 131). This definition already emphasises the adaptive capability, that is not only found in many subsequent definitions (see, e.g. Tukamuhabwa *et al*., 2015; Levalle and Nof, 2017; Kochan and Nowicki, 2018; Ribeiro and Barbosa-Povoa, 2018), but also presents an explicit link to the sensing, seizing and reconfiguration capacities of Dynamic Capability (DC) theory (Pisano and Teece, 1994; Teece *et al*., 1997; Teece, 2007). Recent studies by Silva *et al*. (2022), Stadtfeld and Gruchmann (2023), Scherrer and Doege (2024) and Herburger *et al*. (2024) support this perspective and highlight the critical role of DC in enhancing supply chain resilience.

Scholars have highlighted that resilience can encompass both robust "fail-safe design" and adaptive "safe-fail design" principles (Wieland and Durach, 2021, p. 316). This duality reflects the evolving understanding of SCNR as a systemic and dynamic process rather than a static capability (Yao & and Fabbe-Costes, 2018). In this context, Yao and Fabbe-Costes (2018) conceptualise resilience as comprising three key capabilities: absorbing, responding and capitalising on disruptions. Resilience can also be viewed along a temporal dimension, encompassing four interrelated phases: preparedness, response and recovery and adaptation for the future (Zhao *et al*., 2024). Together, these perspectives underscore that effective SCNR depends on a combination of equilibrium-oriented design choices and adaptive, learning-driven mechanisms that evolve in response to a changing environment.

Recent works often use the term "supply chain network resilience" (SCNR) to emphasise that modern supply chains form complex networks (Kim *et al*., 2015; Li and Zobel, 2020) rather than simple linear chains. This shift in terminology reflects the fact that disruptions may not be contained locally (Ivanov *et al*., 2019), but happen to propagate throughout the entire supply chain network (Li and Zobel, 2020) via the ripple effect (Ivanov *et al*., 2014, 2019). Consequently, we adopt the term SCNR in this contribution.

Research has highlighted the fact that SCNR is fundamentally shaped by two key factors: Network structure (or topology) and node-specific risk capacities (Li and Zobel, 2020). These

elements not only influence how risks propagate but also determine the emergence and characteristics of resilient behaviour (Li and Zobel, 2020). In particular, supply network topology plays a central role in disruption management: While centralised networks are especially vulnerable at key hubs, decentralised structures provide redundancy and flexible rerouting options that help sustain operations during disruptions (Habibi *et al*., 2025). Despite these insights, research on network structures still often assumes node homogeneity (Li *et al*., 2021; Habibi *et al*., 2025), deployed idealised or generic topologies, as, for example in Li and Zobel (2020), Yao *et al.* (2023) or Wang *et al.* (2024) and has insufficiently addressed how disruptions propagate and eventually dissipate in complex networks (Habibi *et al*., 2025).

Fundamental to establishing SCNR is supply chain visibility (Scholten and Schilder, 2015), understood as the availability of multi-tier, upstream and downstream, operational supply network data to the focal firm (Sodhi and Tang, 2019). Visibility is distinct from transparency, that is. the disclosure of product- and operations-related information to external stakeholders such as consumers or investors (Sodhi and Tang, 2019). In the context of this study, visibility determines the extent to which the network's structural properties can be recognised and translated into targeted protective actions (i.e. node fortification; Basole and Bellamy, 2014; Li and Zobel, 2020), even without availability of a complete supply network map (Basole and Bellamy, 2014). This is possible because locally observable structural properties, such as the number of direct ties (i.e. node degree), provide low-information proxies for node criticality, allowing firms to prioritise protection even when only parts of the network are known. Further, visibility enables sensing of potential ripple effect pathways and supports coordinated cross-network fortification strategies (Li and Zobel, 2020). We define "node fortification" as the selective enhancement of a node's disruption resistance and recovery capability through managerial interventions (i.e. multi-sourcing to enable sufficient flow of material to the focal site, capacity buffers and safety stocks at the site, alternative logistics routes to and from the site, data-sharing to enable informed decisions of the site, joint contingency planning between sites to ensure ready-to-execute mitigation plans; Ivanov *et al*., 2019). These concrete instruments align with the broader categories discussed in literature, namely redundancy investments, decentralisation approaches and scenario-based planning (Hart Nibbrig *et al*., 2025), as well as collaboration, relationship management and information sharing (Habibi *et al*., 2025). In our framing, we organise them under two operational levers, redundancy and communication, which we map to the simulation as increased disruption resistance and faster recovery of fortified nodes (Li and Zobel, 2020). Node fortification improves network-level resilience not by altering the topology but by raising local disruption thresholds and shortening downtimes (Li and Zobel, 2020), thus dampening ripple-effect propagation.

Viewed through the Dynamic Capabilities (DC) lens (Pisano and Teece, 1994; Teece *et al*., 1997; Teece, 2007), node fortification operationalises the continuous sensing–seizing–reconfiguration process (see, e.g. Herburger *et al*., 2024): Given a sufficient degree of visibility, sensing identifies structurally critical nodes, seizing targets protective investments at these nodes and reconfiguration revises priorities as the network evolves and risk profiles change. This reflects an internal (Teece, 2007), supply-network-structural sensing perspective (i.e. determining which nodes to fortify given the observable topology and flows). It complements (and does not replace) external sensing (Teece, 2007; Ridder, 2013) of environmental shifts (i.e. demand/supply shocks, regulatory and geopolitical changes), which informs when node fortification should be prepared or adjusted. In turn, DC's sensing–seizing–reconfiguration process naturally integrates into the concept of SCNR (Herburger *et al*., 2024).

This "adaptive capability of the supply chain to prepare for unexpected events, respond to disruptions, and recover from them" (Ponomarov and Holcomb, 2009, p. 131) is further related to a temporal dimension typically articulated as "preparation", "response", "recovery" and "adaptation" phase (Sheffi and Rice, 2005; Tukamuhabwa *et al*., 2015; G. Zhao *et al*., 2024). In the context of this study, our primary contribution concerns the preparation and adaptation phases of individual nodes in a supply chain network. In preparation, we provide a topology-

informed decision rule to prioritise nodes for fortification under partial or full network visibility, enabling firms to allocate scarce resources ex ante to those (visible) nodes whose protection most effectively dampens the ripple effect. In adaptation, the same rule supports periodic re-ranking and reprioritisation as network structure, risk profiles and visibility evolve, thereby turning post-event learning into the next preparation baseline (Scherrer and Doege, 2024). While response and recovery are represented endogenously in our experiments, that is by triggering a disruption and running the model until full recovery, the added value of our contribution lies in prescribing, which nodes to protect prior to a disruption and how to update that set after a disruption as conditions change.

Node fortification is thus one specific resilience strategy that acts at the node level but yields network-level effects through structural leverage. The effect on SCNR is direct, as node fortification reduces both the depth and the duration of the disruption profile (see Figure 1; Sheffi and Rice, 2005).

3. Methodology

We continue to explore proactive ripple effect mitigation by incorporating heterogeneous node risk capacities, implying that nodes possess varying levels of risk capacity, which allows for a more targeted and efficient allocation of resources, and is therefore considered more effective for SCNR improvement in the context of risk propagation (Li and Zobel, 2020). Given this impracticability of fortifying all nodes in a given network, we focus on selecting a critical subset of nodes to protect the overall network. This approach builds on the conventional idea of detecting critical nodes to ensure overall network stability and conceptually aligns with the critical node detection problem in complex network theory (L. Wang *et al*., 2024). In practice, node fortification can be achieved through various strategies (Habibi *et al*., 2025), and in our model follows the redundancy and communication levers outlined in Chapter 2. Our simulation model abstracts these node-level fortification measures as increased resistance to disruptions (i.e. lower disruption transmissibility) and faster recovery from disruptions (i.e. higher recovery capability).

Our study builds upon the work of Doege and Scherrer (2022) by expanding the simulation experiments from a generic 25-node graph to real-world data from the MSOM dataset (Willems, 2007). This approach addresses former limitations, which stemmed partly from the small network size, leading to only minor variations in the outcomes of different node fortification strategies, and partly from the use of a single generic random network structure,

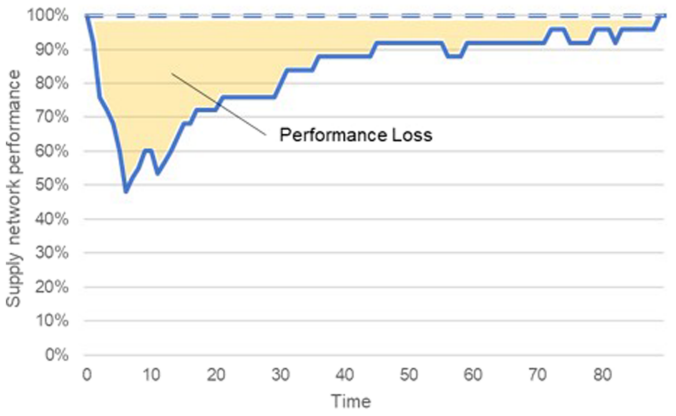

Figure 1. Example of initial disruption and disruption propagation throughout a network. *Source*: Authors' own creation, based on the disruption profile conceptualisation by Sheffi and Rice (2005).

which inevitably abstracts from the complexities of real-world supply chain networks. The MSOM dataset (Willems, 2007) contains supply chain networks from various industries, offering a more realistic perspective as the abstracted network used in Doege and Scherrer (2022), providing deeper insights into SCNR and disruption mitigation strategies.

We implement our simulation experiments using AnyLogic, a widely used multi-method simulation platform. Supply chains are modelled as undirected graphs, where nodes represent supply chain network entities, and edges represent their relationships, aligning with the complex network perspective on supply chains (Wang and Zhang, 2022). Agent-based modelling is particularly well-suited for this context, as it enables decentralised, node-level behaviour. In this modelling approach each node is an autonomous agent, allowing dynamic interaction between agents. This is essential for realistically simulating disruption propagation and local recovery dynamics in complex (supply chain) networks. Furthermore, this approach allows for heterogeneous node characteristics. To simulate disruption propagation and recovery, we apply the general SIR model from epidemiology (Bailey, 1975), but adapted for supply chain networks, as done by, for example, Basole and Bellamy (2014) or Li and Zobel (2020). This is a common approach to modelling risk propagation in complex (supply chain) networks (Brusset *et al*., 2021; Wang *et al*., 2021; Yao *et al*., 2023; Wang *et al*., 2024). In the general SIR model, nodes cycle through three distinct states: Susceptible (S), infected (I) and recovered (R). The process is initiated by a manually introduced initial infection. With a given rate per time unit, infected nodes spread their infection, that is the disruption, to neighbouring nodes that are in susceptible state (Wang and Zhang, 2022). Similarly, infected nodes recover with a given rate per time unit, eventually transitioning into recovered state, in which they are immune to further infection (Wang and Zhang, 2022), resembling mitigation activities and learning effects. As full and permanent immunity to disruptions cannot be achieved in real supply chain networks, we adopt the commonly used SIRS model variant (Wang *et al*., 2021; Wang and Zhang, 2022). In this model, recovered nodes gradually lose their immunity and transition to the susceptible state with a given rate per time unit, allowing for repeated disruption cycles.

We further extend the model by introducing selective node fortification, that is heterogeneous node risk capacities. Fortified nodes resist disruptions with a defined probability and recover more quickly than unfortified nodes. We apply SNA to quantify node importance (or node criticality) and select nodes for fortification, using metrics like betweenness centrality (Bavelas, 1948; Wasserman and Faust, 1994). SNA concepts have been applied to SCM, as demonstrated in the works of Han and Shin (2016) and Zhao *et al*. (2011). A SNA-based approach provides insights into how the structure of supply networks influences both firm-level importance and overall network performance (Kim *et al*., 2011). In addition to betweenness centrality, we use node degree, degree centrality, closeness centrality and page rank to identify the most critical nodes of a network (Doege and Scherrer, 2022). Each of these selection strategies is tested against random fortification to evaluate if (and which) systematic approach to fortifying a subset of a network yields the highest benefit for the resilience of the entire supply chain network. Node degree reflects a node's direct connectivity and is a straightforward indicator of its local importance, nodes with more links are typically more influential in maintaining supply continuity (Hua *et al*., 2025). Degree centrality quantifies how extensively a node is connected within the network, reflecting its relative visibility and influence (Kim *et al*., 2011; Mizgier *et al*., 2013). Nodes with high degree centrality directly affect many others and are structurally more central to network operations (Kim *et al*., 2011; Mizgier *et al*., 2013). Closeness centrality captures how near a node is to all others in the network, including those beyond its direct connections (Kim *et al*., 2011). Nodes with high closeness can quickly reach the entire network, making them more autonomous, more important and less reliant on intermediaries (Kim *et al*., 2011; Hua *et al*., 2025). Betweenness centrality measures how often a node lies on the shortest paths between others, highlighting its role as an intermediary (Kim *et al*., 2011; Mizgier *et al*., 2013; Hua *et al*., 2025). Nodes with high betweenness can control or facilitate interactions between

otherwise unconnected parts of the network, making them structurally influential and potentially critical for network cohesion (Kim *et al*., 2011; Hua *et al*., 2025). Page rank evaluates node importance by considering not only the number of incoming links, but also the importance of the linking nodes (Page *et al*., 1999; Hua *et al*., 2025). It reflects the idea that connections from highly ranked nodes confer greater influence, making it well suited for identifying structurally prominent actors in complex networks (Page *et al*., 1999; Hua *et al*., 2025). In our setting, SNA metrics are selection logics that indicate where to deploy fortification measures. Fortification combines redundancy (i.e. multi-sourcing and/or diversifying sourcing strategies, stockpiling of critical materials, backup manufacturing capacities or establishing alternative logistics routes) and communication (i.e. data and information sharing, early-warning mechanisms, staff training and cross-training across productions sites). For high degree and degree centrality nodes (high connectivity), these measures reduce disruption transmission and increase recovery capability. For high closeness nodes (rapid-reach nodes) and betweenness nodes (bridges between subnetworks), fortification aims to interrupt transfers across subnetworks and accelerate reconnection of separated parts of the network. For high page rank nodes (influence hubs), fortification dampens amplification at the source, lowering the likelihood that local shocks escalate into network-wide losses. A summary of the SNA-based node-selection logics and their mapping to fortification objectives is presented in Table 1.

These SNA measures, applied to the MSOM dataset's real networks (Willems, 2007), enable a more practical analysis compared to the generic and significantly smaller graph used by Doege and Scherrer (2022). We perform our simulation experiments on a subset of the MSOM Dataset (Willems, 2007). The dataset contains 38 supply chains from various industries, ranging from 8 to 2025 nodes. We select a subset of 10 medium-sized networks and define 150 nodes as the minimum threshold to ensure that we select sufficiently large networks to overcome some of the limitations associated with the rather small network size of the preceding work of Doege and Scherrer (2022). An overview of our subset is presented in Table 2.

For each of the 10 networks, we perform two types of experiments: One simulating disruptions to a single node and the other simulating simultaneous disruptions to multiple nodes. This approach represents low-frequency, high-impact events like natural disasters, pandemics or geopolitical events (Li and Zobel, 2020), as well as severe planning errors or equipment breakdown, with single- and multi-node disruptions capturing varying degrees of

Table 1. Summary of SNA-based node-selection logics and mapping to fortification objectives

Node-selection logic	Interpretation	Fortification objective
Node degree	Quantifies direct links; more links = more immediate connectivity	Maintain operational continuity + prevent disruption spread via connected/important node(s)
Degree centrality	Quantifies node's connections relative to whole network	Maintain operational continuity + prevent disruption spread via relatively connected/ important node(s)
Closeness centrality	Quantifies how quickly a node can reach all others	Maintain operational continuity + prevent disruption spread via gateway node(s)
Betweenness centrality	Quantifies how often a node is in the shortest path between other nodes	Maintain operational continuity + prevent disruption spread via intermediary/bridging node(s)
Page rank	Quantifies a node's influence by weighting incoming links by the influence of their sources	Maintain operational continuity + prevent disruption spread at influential hub node(s)

Source(s): Kim *et al*. (2011), Mizgier *et al*. (2013), Hua *et al*. (2025), Page *et al*. (1999)

Table 2. Networks considered for simulation experiments

Supply chain	Industry	Nodes	Edges	Average degree
MSOM 18	Computer Peripheral Equipment, Not Elsewhere Classified	154	224	2.91
MSOM 19	Computer Peripheral Equipment, Not Elsewhere Classified	156	263	3.37
MSOM 20	Computer Peripheral Equipment, Not Elsewhere Classified	156	169	2.17
MSOM 21	Perfumes, Cosmetics and Other Toilet Preparations	186	359	3.86
MSOM 22	Pharmaceutical Preparations	253	253	2.00
MSOM 23	Paints, Varnishes, Lacquers, Enamels and Allied Products	271	524	3.87
MSOM 24	Power-Driven Handtools	334	1,245	7.46
MSOM 25	Farm Machinery and Equipment	409	853	4.17
MSOM 26	Aircraft Engines and Engine Parts	468	605	2.59
MSOM 27	Electromedical and Electrotherapeutic Apparatus	482	941	3.90

Source(s): Willems (2007)

disruption intensity. Resilience is evaluated by measuring the depth of the dip in performance (i.e. the number of non-operational nodes during disruption propagation) and the length of the dip (i.e. time to full recovery). Both constitute the performance loss (Munoz and Dunbar, 2015), which is the area between regular performance and the performance curve during disruption (i.e. the highlighted area in Figure 1). A more resilient, or fortified, supply chain network exhibits a shallower performance dip and/or a quicker recovery and thus a smaller performance loss. Conversely, a deeper and longer dip in performance indicates a less resilient supply chain network.

4. Results

On each of the 10 selected supply chains we perform a set of simulation experiments to measure the effect of selective node fortification over unfortified networks. We analyse five SNA parameters to identify the most critical nodes in a network and test these fortification strategies against a random selection and fortification of nodes. We fortify the nodes in two dimensions: Their ability to withstand disruptions and their ability to quickly return to an operational state when disrupted. The ability to withstand disruptions corresponds to a reduced infection probability within the SIR model, whereas the ability to return to an operational state more quickly translates into a faster recovery rate compared to unfortified nodes. For fortified and unfortified networks, we test two types of disruptions, that is a small single node being initially disrupted, and a larger 20% multi-node initial disruption. We use these two shock scenarios to represent typical disruption scales. A single-node disruption represents local events (i.e. a plant fire, cyber outage, catastrophic machine failure) that may still ripple through the network (Sheffi and Rice, 2005; Li and Zobel, 2020). A 20% multi-node disruption approximates events that impact many nodes at once within a region or tier (i.e. earthquake, flood, pandemic lockdowns, sanctions) (Ivanov *et al*., 2019; Habibi *et al*., 2025). Choosing 20% creates a severe, yet plausible, stress for the considered networks. Using both types of disruptions allows to contrast the effectiveness of fortification under local and systemic onset and to test for potential non-linearities in the benefit of targeted node fortification.

Consequently, in total we perform $10 * (5 + 1) * 2 * 2 = 240$ simulation instances. Every instance of the simulation experiment is repeated 100 times to average out random variations in the disruption propagation process.

Our findings demonstrate that irrespective of the configuration of the real-world network, any fortification strategy consistently proves advantageous in mitigating the adverse impact of disruption on performance. It can be observed that targeted fortification is, in general, more effective than random fortification: In case of single-node disruptions and random fortification

of nodes, the performance loss is reduced by 34.49% on average (see Figure 2). Targeted fortification leads to an average performance loss reduction of 69.56%, compared to the unfortified case. In instances of multi-node disruptions, we observe comparable results. With random fortification, the performance loss is on average reduced by 13.93%, compared to the unfortified case. Targeted fortification on average delivers a performance loss that is 28.57% smaller that in case of no fortification.

A detailed examination of fortification strategies reveals that in one of the ten cases (i.e. MSOM 26), closeness centrality demonstrates inferior performance compared to random fortification. Conversely, in all other cases, SNA-based strategies exhibit superior outcomes compared to random fortification. Among the SNA-based strategies, fortifying nodes based on page rank appears to result in the greatest reduction of disruption-related losses. Overall, the SNA-based strategies perform similarly, as shown in Figure 3, and consistently outperform random fortification.

5. Discussion

While our results clearly confirm that targeted node fortification consistently outperforms random fortification in mitigating the impact of supply chain disruptions, a deeper examination of the results reveals important differences between the selection strategies. In particular, we find that node fortification based on page rank tends to provide the greatest SCNR benefits in our simulation experiments. However, simpler SNA metrics such as node degree, betweenness and closeness centrality provide comparable performance improvements in most cases.

This relatively small performance gap between advanced and basic network metrics such as node degree has important managerial implications. In practice, firms often face limited visibility into their supply networks (Bowen and Siegler, 2024), making complex or data-intensive metrics such as page rank difficult to implement. Our findings suggest that even when complete network information is not available, relying on simpler and more accessible measures such as node degree can yield significant SCNR benefits. High-degree nodes both receive from and feed many neighbouring nodes. Fortifying high-connectivity nodes removes/insulates a large fraction of potential disruption transmission (i.e. ripple effect) corridors and accelerates overall recovery along the two major levers redundancy and communication. Redundancy (i.e. multi-sourcing and/or diversifying sourcing strategies, stockpiling of critical materials, backup manufacturing capacities or establishing alternative logistics routes) lowers both effective transmissibility by reducing dependence on any single disrupted node or link and raises recovery capability by providing spare resources/capacities that can be activated quickly. Communication (i.e. data and information sharing, early-warning mechanisms, staff

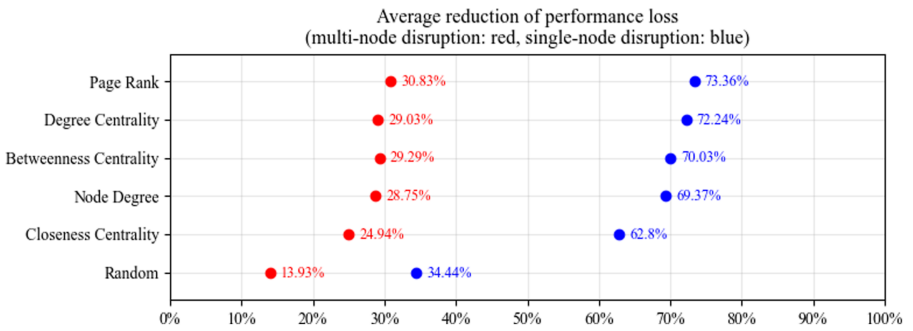

Figure 2. Average reduction of performance loss per node selection strategy across all considered MSOM networks

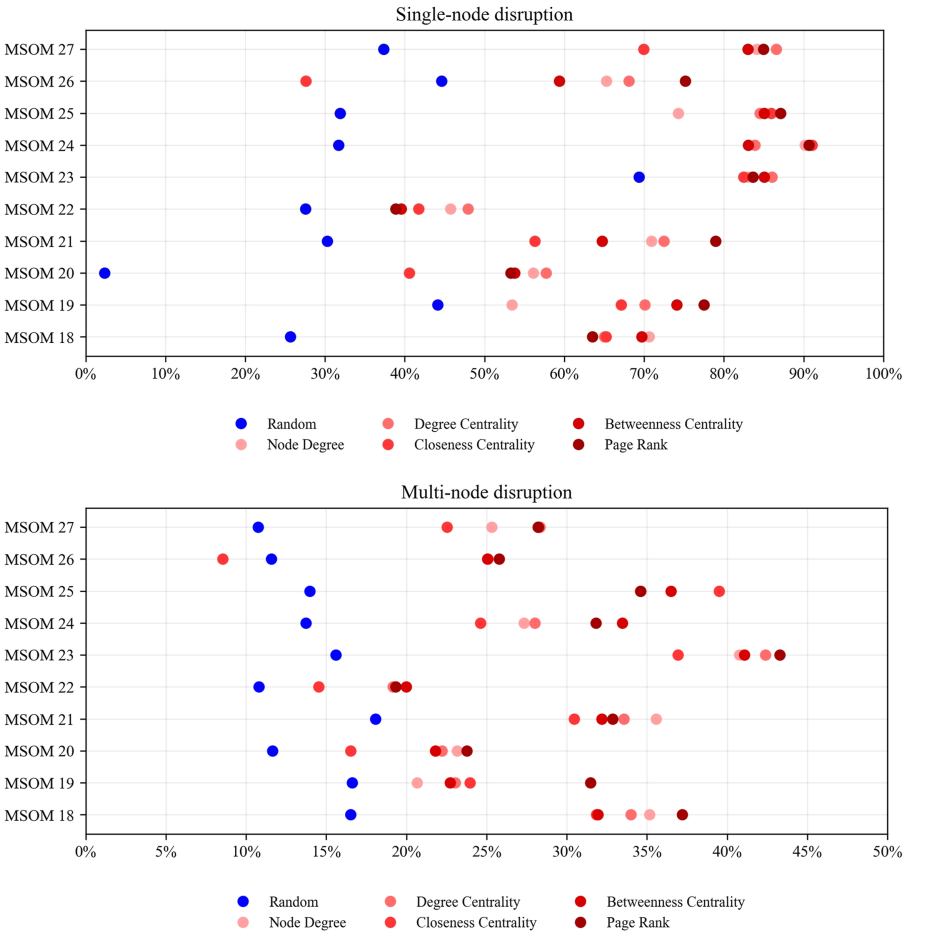

Figure 3. Average reduction of performance loss per node fortification strategy on different MSOM networks

training and cross-training across productions sites) primarily reduces effective transmissibility through faster detection, triage and coordinated containment, while also increasing recovery capability by enabling quicker, better-orchestrated recovery. Strengthening these practices at highly connected nodes improves signal quality (what is happening, where and when) and accelerates coordinated action across many nodes simultaneously, which explains the network-level effect of fortifying a small set of high-degree nodes. In this way, firms can enhance SCNR without necessarily requiring full network visibility or sophisticated analytical capabilities.

Moreover, while all SNA-based strategies generally outperform random fortification, the marginal differences between them suggest that strategy selection should be context-specific. In supply networks where complete information is available and computational resources are sufficient, prioritising nodes based on page rank may provide maximum SCNR improvements. In such high-visibility settings, influence-aware metrics provide additional leverage. Page rank highlights amplifier nodes, that aggregate exposure from already influential neighbouring nodes. Betweenness centrality highlights gatekeepers/bridges through which disruptions cross from one subnetwork to another. Fortifying nodes with high page rank reduces amplification at

influential hubs, thereby lowering effective transmissibility. Fortifying nodes with high betweenness centrality removes or insulates major disruption transmission corridors between subnetworks and accelerates overall recovery. The additional network-level benefit is explained by the concentration of fortification efforts where they matter most: At nodes that serve as bridges between subnetworks (i.e. nodes with high betweenness centrality). Both fortification strategies, selecting nodes by page rank or betweenness centrality, are operationalised through the same two levers: Redundancy and communication. Conversely, in settings where data availability is limited or the use of simple metrics is required, selecting nodes for fortification based on their degree provides a highly effective and pragmatic alternative.

These findings also extend and refine conclusions drawn by Doege and Scherrer (2022), which was based on a generic 25-node random network. Despite its abstract nature, that study delivered three key insights: (1) selective node fortification improves overall network performance; (2) systematic fortification strategies outperform random node selection and (3) the tested SNA-based node selection methods produced broadly similar outcomes. However, no single SNA metric consistently outperformed the others. In contrast, the present study, based on large-scale, real-world networks, demonstrates that page rank consistently provides superior results across all tested scenarios, thereby providing clearer guidance for practical applications of SNA-based fortification strategies. In practice, firms can match the metric to the information environment: Use page rank (or betweenness centrality) where a more global, multi-tier network visibility is available, and node degree where only local information exist. In both cases fortify the highest ranked nodes via redundancy or communication levers.

From a managerial process integration perspective, our results advocate for embedding network analysis into existing supply chain risk management practices. Simple measures like node degree could be operationalised through regular supplier audits or digital supply chain mapping initiatives, enabling firms to identify and fortify critical nodes proactively. For more digitally mature organisations, advanced analytics could extend this by incorporating more complex measures like page rank into digital twins of supply networks to continually reassess node criticality as network structures evolve. Our managerial takeaways are consistent with interview evidence reported by Scherrer and Doege (2024), where respondents described adjustments before, during and after disruptive events. Read through the DC lens, these actions instantiate sensing, seizing and reconfiguration (Teece *et al*., 1997; Teece, 2007).

From a theory perspective, we conclude that the resilience benefit of a node-selection logic is conditional on information availability. With limited visibility, local structural information (i.e. node degree) is sufficient, but with a richer multi-tier insight, global influence (i.e. page rank) delivers a resilience benefit premium. We further conclude that node fortification acts locally, but generates a system-level loss reduction, clarifying that node-level capabilities translate into SCNR outcomes without altering network topology.

The underperformance of closeness centrality (MSOM 26) is consistent with this view: When the ripple effect mainly passes through a few gatekeeper nodes that bridge otherwise separate parts of the network, being centrally located (i.e. closeness centrality) matters less than being in a bridging position. In such cases, influence-based ranking (i.e. page rank or betweenness centrality) identifies the right bridging nodes for fortification and therefore outperforms proximity-based ranking (i.e. closeness centrality).

Viewed through the lens of DC (Teece *et al*., 1997; Teece, 2007; Herburger *et al*., 2024), our findings suggest a sensing premium, specifically in the sense of internal, supply-network-structural sensing, meaning that when sensing can draw on richer multi-tier visibility and thus prioritise nodes using more global influence signals (i.e. page rank) rather than only local influence signals (i.e. node degree), the resilience payoff of node fortification increases. This internal sensing perspective (i.e. determining which nodes to fortify given observable topology and flows) complements (and does not replace) external sensing of environmental shifts, which informs when node fortification should be prepared or adjusted. In our results the increased resilience payoff is shown by page rank consistently providing superior results

where visibility is higher, while degree remains a robust low-information alternative for partial visibility.

In DC terms, sensing determines the ranking of nodes given the current visibility, seizing efficiently allocates fortification to the prioritised set of nodes and reconfiguration updates this set of nodes as network structure and exposure levels evolve:

(1) Sensing (internal and external): Internal sensing identifies (within the visible network) the nodes whose fortification yields the largest overall resilience benefit for the entire network. Depending on visibility, different influence signals (i.e. page rank or node degree) may be deployed to identify those critical nodes. External sensing tracks environmental signals (i.e. demand/supply shocks, regulatory and geopolitical changes) and thereby informs the timing for fortification. Together, internal and external sensing determine which nodes to prioritise and when to perform the fortification.

(2) Seizing (targeted allocation): Seizing translates the node prioritisation into fortification measures at the selected nodes via the levers redundancy (i.e. multi-sourcing and/or diversifying sourcing strategies, stockpiling of critical materials, backup manufacturing capacities or establishing alternative logistics routes) and communication (i.e. data and information sharing, early-warning mechanisms, staff training and cross-training across productions sites).

(3) Reconfiguration (adaptive reprioritisation): Reconfiguration updates the priority as network structure, risk exposures and network visibility evolve: Re-rank nodes on a regular basis (i.e. yearly), reduce fortification at de-prioritised nodes and scale up fortification at newly critical nodes.

This combination of internal/external sensing, targeted seizing and continuous reconfiguration sustains resilience as the network changes.

In sum, while the overall advantage of targeted fortification might seem intuitive, our findings emphasise the fact that even basic, easily implementable strategies (i.e. fortification based on node degree) can significantly enhance SCNR. Choosing the appropriate fortification approach, that is relying on local connectivity information such as node degree versus using global influence signals such as page rank, should balance expected SCNR benefits with data availability, analytical capabilities and urgency of the decision context.

6. Conclusion and further research

Our study highlights the effectiveness of network fortification strategies in mitigating adverse impacts of supply chain disruptions, with targeted fortification consistently outperforming random fortification. Across both single-node and multi-node disruptions, targeted approaches reduce performance loss, proving that strategic interventions enhance SCNR regardless of the specific configuration of the supply network.

While targeted fortification consistently outperforms random fortification, our findings reveal nuanced differences among selection strategies: Page rank generally offers the greatest SCNR benefits, but simpler metrics like node degree, betweenness or closeness centrality achieve comparable results. This suggests that even low network visibility can enable effective SCNR strategies, particularly important in contexts where full network mapping is impractical. Given the minimal performance difference, managers can confidently use simpler metrics like node degree to identify key nodes for fortification, making the approach both practical and efficient for enhancing SCNR. In conclusion, our findings emphasise that targeted fortification strategies significantly reduce the impact of disruptions, regardless of the method used. The small performance gap between different SNA-based approaches highlights that even simple, easily implemented strategies like node degree are highly effective, making them valuable tools for practitioners in fortifying supply networks.

Regarding theory, we link visibility and information conditions to SCNR outcomes. We further ground node fortification in DC, showing how sensing, seizing and reconfiguration translate into measurable reductions in disruption depth and duration on real-world networks. In short, the resilience benefit of a node fortification logic is conditional on visibility. With limited visibility, local network or connectivity information (i.e. node degree) is sufficient. With richer, multi-tier insight, global influence signals (i.e. page rank) deliver an additional resilience premium. This perspective explains why influence-based node fortification dominates with increased visibility, while node degree remains a simple and robust alternative. This further clarifies our theory contribution: A conditional, DC-based explanation of how information conditions shape the effectiveness of topology-informed node fortification to enhance SCNR.

While the use of real-world networks significantly enhances the practical relevance of this study, the relatively small sample size remains a limitation. Future research could expand the sample to include more supply chains to control for industry-specific or network structural characteristics. Furthermore, while our analysis primarily focused on nodes and edges as structural elements, supply chains are inherently heterogeneous in other aspects that can significantly influence the dynamics of disruption propagation and resilience. As our results show, even supply chains with similar structural descriptions, such as MSOM 18 and MSOM 19, can yield different results. Future studies should therefore aim to characterise and cluster supply chains more comprehensively, considering additional factors beyond the basic network structure. This would enable a deeper understanding of the underlying drivers of SCNR and allow more tailored fortification strategies to be developed. Expanding the dataset and incorporating more supply chain attributes would also help to further validate the generalisability of our findings. In the study at hand, we emphasised that supply network resilience can be positively influenced by the adoption of DC. Two things are missing, which could be used to shape future's avenue towards higher levels of SCNR. First, path dependency should be taken into consideration when selecting actions to fortify certain nodes. Second not only DC, but also complex adaptive systems, which lead to different decision, should be taken into consideration. If a company leans on DC different decisions are made in node fortification than if a network is understood as a complex adaptive system.

References

Bailey, N.T. (1975), "The mathematical theory of infectious diseases and its applications".

Basole, R.C. and Bellamy, M.A. (2014), "Supply network structure, visibility, and risk diffusion: a computational approach", *Decision Sciences*, Vol. 45 No. 4, pp. 753-789, doi: 10.1111/deci.12099.

Bavelas, A. (1948), "A mathematical model for group structures", *Human Organization*, Vol. 7 No. 3, pp. 16-30, doi: 10.17730/humo.7.3.f4033344851gl053.

Bowen, F. and Siegler, J. (2024), "The role of visibility in supply chain resiliency: applying the Nexus supplier index to unveil hidden critical suppliers in deep supply networks", *Decision Support Systems*, Vol. 176, 114063, doi: 10.1016/j.dss.2023.114063.

Brusset, X., Davari, M., Kinra, A. and Torre, D.L. (2021), "Modelling COVID-19 ripple effect and global supply chain productivity impacts using a reaction-diffusion time-space SIS model", in Dolgui, A., Bernard, A., Lemoine, D., von Cieminski, G. and Romero, D. (Eds), *Advances in Production Management Systems. Artificial Intelligence for Sustainable and Resilient Production Systems*, Springer International Publishing, pp. 3-12, doi: 10.1007/978-3-030-85910-7_1.

Chopra, S. and Sodhi, M.S. (2004), "Supply-chain breakdown", *MIT Sloan Management Review*, Vol. 46 No. 1, pp. 53-61, available at: https://sloanreview.mit.edu/article/managing-risk-to-avoid-supplychain-breakdown/

Christopher, M. and Peck, H. (2004), "Building the resilient supply chain", *The International Journal of Logistics Management*, Vol. 15 No. 2, pp. 1-14, doi: 10.1108/09574090410700275.

Doege, P. and Scherrer, M. (2022), "Systematic node fortification to mitigate the ripple effect and increase supply chain network resilience", *29th International Annual EurOMA Conference*, Berlin, Germany, 1-6 July 2022, available at: https://digitalcollection.zhaw.ch/handle/11475/26218

Habibi, F., Chakrabortty, R.K., Abbasi, A. and Ho, W. (2025), "Investigating disruption propagation and resilience of supply chain networks: interplay of tiers and connections", *International Journal of Production Research*, Vol. 63 No. 17, pp. 1-23, doi: 10.1080/00207543.2025.2470348.

Han, J. and Shin, K. (2016), "Evaluation mechanism for structural robustness of supply chain considering disruption propagation", *International Journal of Production Research*, Vol. 54 No. 1, pp. 135-151, doi: 10.1080/00207543.2015.1047977.

Hart Nibbrig, M., Sharif Azadeh, S. and Maknoon, M.Y. (2025), "Adaptive resilience strategies for supply chain networks against disruptions", *Transportation Research Part E: Logistics and Transportation Review*, Vol. 200, 104172, doi: 10.1016/j.tre.2025.104172.

Herburger, M., Wieland, A. and Hochstrasser, C. (2024), "Building supply chain resilience to cyber risks: a dynamic capabilities perspective", *Supply Chain Management: An International Journal*, Vol. 29 No. 7, pp. 28-50, doi: 10.1108/SCM-01-2023-0016.

Hua, Z., Xia, Y., Chen, Y. and Sun, W. (2025), "Identification of critical nodes in supply chain networks", *AIP Advances*, Vol. 15 No. 1, 015224, doi: 10.1063/5.0249078.

Ivanov, D. (2018), "Supply chain management and structural dynamics control", in Ivanov, D. (Ed.), *Structural Dynamics and Resilience in Supply Chain Risk Management*, Springer International Publishing, pp. 1-18, doi: 10.1007/978-3-319-69305-7_1.

Ivanov, D., Sokolov, B. and Dolgui, A. (2014), "The Ripple effect in supply chains: trade-off 'efficiency-flexibility-resilience' in disruption management", *International Journal of Production Research*, Vol. 52 No. 7, pp. 2154-2172, doi: 10.1080/00207543.2013.858836.

Ivanov, D., Dolgui, A. and Sokolov, B. (Eds) (2019), *Handbook of Ripple Effects in the Supply Chain*, Springer International Publishing, Vol. 276, doi: 10.1007/978-3-030-14302-2.

Kim, Y., Choi, T.Y., Yan, T. and Dooley, K. (2011), "Structural investigation of supply networks: a social network analysis approach", *Journal of Operations Management*, Vol. 29 No. 3, pp. 194-211, doi: 10.1016/j.jom.2010.11.001.

Kim, Y., Chen, Y.-S. and Linderman, K. (2015), "Supply network disruption and resilience: a network structural perspective", *Journal of Operations Management*, Vols 33-34 No. 1, pp. 1-59, doi: 10.1016/j.jom.2014.10.006.

Kochan, C.G. and Nowicki, D.R. (2018), "Supply chain resilience: a systematic literature review and typological framework", *International Journal of Physical Distribution & Logistics Management*, Vol. 48 No. 8, pp. 842-865, doi: 10.1108/ijpdlm-02-2017-0099.

Levalle, R.R. and Nof, S.Y. (2017), "Resilience in supply networks: definition, dimensions, and levels", *Annual Reviews in Control*, Vol. 43, pp. 224-236, doi: 10.1016/j.arcontrol.2017.02.003.

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

Li, Y., Chen, K., Collignon, S. and Ivanov, D. (2021), "Ripple effect in the supply chain network: forward and backward disruption propagation, network health and firm vulnerability", *European Journal of Operational Research*, Vol. 291 No. 3, pp. 1117-1131, doi: 10.1016/j.ejor.2020.09.053.

Mizgier, K.J., Jüttner, M.P. and Wagner, S.M. (2013), "Bottleneck identification in supply chain networks", *International Journal of Production Research*, Vol. 51 No. 5, pp. 1477-1490, doi: 10.1080/00207543.2012.695878.

Munoz, A. and Dunbar, M. (2015), "On the quantification of operational supply chain resilience", *International Journal of Production Research*, Vol. 53 No. 22, pp. 6736-6751, doi: 10.1080/00207543.2015.1057296.

Page, L., Brin, S., Motwani, R. and Winograd, T. (1999), "The PageRank citation ranking: bringing order to the web", [Techreport]. Stanford InfoLab, available at: http://ilpubs.stanford.edu:8090/422/?utm_campaign=Technical%20SEO%20Weekly&utm_medium=email&utm_source=Revue%20newsletter

Pisano, G. and Teece, D.J. (1994), "The dynamic capabilities of firms: an introduction", *Industrial and Corporate Change*, Vol. 3 No. 3, pp. 3-556, doi: 10.1093/icc/3.3.537-a.

Ponomarov, S.Y. and Holcomb, M.C. (2009), "Understanding the concept of supply chain resilience", *The International Journal of Logistics Management*, Vol. 20 No. 1, pp. 124-143, doi: 10.1108/09574090910954873.

Ribeiro, J.P. and Barbosa-Povoa, A. (2018), "Supply Chain Resilience: definitions and quantitative modelling approaches – a literature review", *Computers and Industrial Engineering*, Vol. 115, pp. 109-122, doi: 10.1016/j.cie.2017.11.006.

Rice, J.B. and Caniato, F. (2003), "Building a secure and resilient supply network", *Supply Chain Management Review*, Vol. 7 No. 5, pp. 22-33.

Ridder, A.K. (2013), "External dynamic capabilities: competitive advantage in innovation via external resource renewal", in *Academy of Management Proceedings*, Academy of Management, Briarcliff Manor, NY, Vol. 2013 No. 1, 10356.

Scherrer, M. and Doege, P. (2024), "The influencing role of supply chain understanding and disruption perception on supply chain network resilience", *31st European Operations Management Association (EurOMA)*, Sant Cugat, Spain, 29 June, available at: https://digitalcollection.zhaw.ch/items/cfc87ced-6419-4021-b59b-23a477e53263 (accessed 4 July 2024).

Scholten, K. and Schilder, S. (2015), "The role of collaboration in supply chain resilience", *Supply Chain Management: An International Journal*, Vol. 20 No. 4, pp. 471-484, doi: 10.1108/SCM-11-2014-0386.

Sheffi, Y. and Rice, J.B.J. (2005), *A Supply Chain View of the Resilient Enterprise*, MIT Sloan Management Review, available at: https://sloanreview.mit.edu/article/a-supply-chain-view-of-the-resilient-enterprise/

Silva, M.E., Pereira, M.M.O. and Hendry, L.C. (2022), "Embracing change in tandem: resilience and sustainability together transforming supply chains", *International Journal of Operations & Production Management*, Vol. 43 No. 1, pp. 166-196, doi: 10.1108/IJOPM-09-2022-0625.

Sodhi, M.S. and Tang, C.S. (2019), "Research opportunities in supply chain transparency", *Production and Operations Management*, Vol. 28 No. 12, pp. 2946-2959, doi: 10.1111/poms.13115.

Stadtfeld, G.M. and Gruchmann, T. (2023), "Dynamic capabilities for supply chain resilience: a meta-review", *The International Journal of Logistics Management*, Vol. 35 No. 2, pp. 623-648, doi: 10.1108/IJLM-09-2022-0373.

Teece, D.J. (2007), "Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance", *Strategic Management Journal*, Vol. 28 No. 13, pp. 13-1350, doi: 10.1002/smj.640.

Teece, D.J., Pisano, G. and Shuen, A. (1997), "Dynamic capabilities and strategic management", *Strategic Management Journal*, Vol. 18 No. 7, pp. 7-533, doi: 10.1002/(sici)1097-0266(199708)18:7<509::aid-smj882>3.0.co;2-z.

Tukamuhabwa, B.R., Stevenson, M., Busby, J. and Zorzini, M. (2015), "Supply chain resilience: definition, review and theoretical foundations for further study", *International Journal of Production Research*, Vol. 53 No. 18, pp. 5592-5623, doi: 10.1080/00207543.2015.1037934.

Wang, H. and Zhang, X. (2022), "Research on supply chain risk transmission mechanism based on improved SIRS model", *Mathematical Problems in Engineering*, Vol. 2022 No. 1, pp. 9502793-9502799, doi: 10.1155/2022/9502793.

Wang, J., Zhou, H. and Jin, X. (2021), "Risk transmission in complex supply chain network with multi-drivers", *Chaos, Solitons and Fractals*, Vol. 143, 110259, doi: 10.1016/j.chaos.2020.110259.

Wang, L., Yao, F., Wu, Z. and Gao, R. (2024), "Simulation system design for critical-node detection and robustness analysis of supply chains", *Enterprise Information Systems*, Vol. 18 No. 5, 2326673, doi: 10.1080/17517575.2024.2326673.

Wasserman, S. and Faust, K. (1994), "Social network analysis: methods and applications", available at: https://www.cambridge.org/de/universitypress/subjects/sociology/sociology-general-interest/social-network-analysis-methods-and-applications?format=PB&isbn=9780521387071

Wieland, A. and Durach, C.F. (2021), "Two perspectives on supply chain resilience", *Journal of Business Logistics*, Vol. 42 No. 3, pp. 315-322, doi: 10.1111/jbl.12271.

Willems, S.P. (2007), "Data set—real-world multiechelon supply chains used for inventory optimization", *Manufacturing & Service Operations Management*, Vol. 10 No. 1, pp. 19-23, doi: 10.1287/msom.1070.0176.

Yao, Y. and Fabbe-Costes, N. (2018), "Can you measure resilience if you are unable to define it? The analysis of Supply Network Resilience (SNRES)", *Supply Chain Forum: International Journal*, Vol. 19 No. 4, pp. 255-265, doi: 10.1080/16258312.2018.1540248.

Yao, Q., Fan, R., Chen, R. and Qian, R. (2023), "A model of the enterprise supply chain risk propagation based on partially mapping two-layer complex networks", *Physica A: Statistical Mechanics and its Applications*, Vol. 613, 128506, doi: 10.1016/j.physa.2023.128506.

Zhao, K., Kumar, A., Harrison, T.P. and Yen, J. (2011), "Analyzing the resilience of complex supply network topologies against random and targeted disruptions", *IEEE Systems Journal*, Vol. 5 No. 1, pp. 28-39, doi: 10.1109/JSYST.2010.2100192.

Zhao, G., Vazquez-Noguerol, M., Liu, S. and Prado-Prado, J.C. (2024), "Agri-food supply chain resilience strategies for preparing, responding, recovering, and adapting in relation to unexpected crisis: a cross-country comparative analysis from the COVID-19 pandemic", *Journal of Business Logistics*, Vol. 45 No. 1, e12361, doi: 10.1111/jbl.12361.

Corresponding author
Patrick Doege can be contacted at: patrick.doege@outlook.de