ACCSCIENCE PUBLISHING

Asian Journal of Water, Environment and Pollution

ORIGINAL RESEARCH ARTICLE

Energy transition and industrial supply chain security: Propagating mechanisms of carbon reduction risks in manufacturing networks

Yu He[1], Si Qin Shu[1], Zhen Zhen Chen[1]*, and Jie Xin Tian[2]

[1]Department of Economics, College of Economics and Management, China Three Gorges University, Yichang, Hubei, China

[2]Department of Economics, School of Economics and Management, China University of Geosciences, Wuhan, Hubei, China

(This article belongs to the *Special Issue: Pathways to Carbon Neutrality and Low-Carbon Energy Transition in China: Policy, Technology, and Systemic Innovation*)

Abstract

Global carbon reduction mandates drive the energy transition but expose manufacturing supply chains to carbon reduction risks. This study employs complex network theory to construct a multi-stage industrial chain model, integrating numerical simulations to examine the transmission of carbon reduction risk under random and targeted shocks. Carbon reduction risks raise costs, trigger price increases, and induce risk transmission. Network robustness exhibited structural heterogeneity: random networks outperformed scale-free and small-world networks under random shocks, while small-world networks showed the highest resilience against targeted attacks. Targeted attacks triggered a 50% efficiency loss in scale-free networks at an early attack round, far exceeding the impact of random shocks of the same intensity. Network failure probability was inversely correlated with the strategic resilience parameter and positively correlated with the external dependency parameter: elevating the strategic resilience parameter above 0.5 and maintaining the external dependency parameter below 0.5 significantly enhanced small-world network resilience. Adjusting either parameter alone failed to mitigate cascading failures in scale-free networks under targeted attacks. For random networks, a strategic resilience parameter above 0.3 prevented efficiency from falling below the 50% threshold under random shocks. This study innovates by establishing a benchmark model that links carbon reduction risk dynamics to supply chain network structure, providing a quantitative analytical framework for policymakers to design targeted resilience strategies and for managers to optimize network robustness amid decarbonization pressures.

Keywords: Carbon reduction risk; Supply chain networks; Risk propagation; Complex networks; Cascading failures

***Corresponding author:**
Chen Zhenzhen
(chenzhenzhen@ctgu.edu.cn)

Citation: He Y, Shu SQ, Chen ZZ, Tian JX. Energy transition and industrial supply chain security: Propagating mechanisms of carbon reduction risks in manufacturing networks. *Asian J Water Environ Pollut.* 2026;23(3):026020010. doi: 10.36922/AJWEP026020010

Received: January 10, 2026

Revised: February 27, 2026

Accepted: February 27, 2026

Published online: April 9, 2026

1. Introduction

The escalating global climate crisis has rendered the green transition of energy structures a pressing priority for all nations,[1] and curbing carbon emissions stands as one of the most critical pathways to achieving this transition. However, this imperative introduces substantial risks to manufacturing supply chains.[2] Mounting pressure to reduce carbon emissions has prompted countries to implement low-carbon policies and measures. Firms are consequently compelled to bear additional carbon emission costs in their production processes, such as carbon taxes, emission allowances, and investments in green technologies. This directly poses carbon reduction risks for firms. Firms typically do not operate in isolation. Instead, they are interconnected through complex supply relationships, forming structured supply chain networks. Under this networked organizational model, cost increases, production adjustments, or supply disruptions arising from decarbonization pressures at one firm can cascade through upstream and downstream linkages to affect other firms. These disruptions may trigger cascading effects that jeopardize the operational stability of the entire supply chain.[3] Thus, integrating analysis of carbon reduction risk into the study of pollution mitigation,[4] energy transition,[5] and sustainable development is critical,[6] with supply chain resilience emerging as a core factor in balancing decarbonization goals and industrial continuity.[7]

Efforts to reduce carbon emissions may disrupt carbon-intensive industries, thereby exposing structural vulnerabilities linked to the comparatively limited adaptive capacity of developing economies relative to their advanced counterparts.[8] This challenge is amplified by structural mismatches between the high-carbon energy consumption profile of current manufacturing[9] and low-carbon development objectives, compounded by limited technological and financial capacities.[10] These factors jointly impose dual pressures on emissions control and productivity improvement.[11] Therefore, the pursuit of a low-carbon transition and economic growth entails multidimensional hurdles spanning technological pathways, financial resources, and institutional frameworks.[12]

The sustainable development of the manufacturing sector is further constrained by dual deficiencies in structural optimization and technological advancement.[13] Production processes continue to rely excessively on carbon-intensive energy sources,[14] whereas technological innovation capabilities remain inadequate.[15] This combination reinforces a vicious cycle of excessively high emissions and suboptimal production efficiency.[16] Moreover, premature adoption of aggressive decarbonization measures carries carbon reduction risks.[17] Empirical studies have noted a potential outcome: annual economic growth rates could drop by 1.5 to 2 percentage points.[18] This leads to a "low-carbon poverty paradox."[19] In this paradox, environmental goals come into conflict with poverty alleviation[20] and basic developmental needs.[21]

From an industrial chain perspective,[22] low-carbon technology development may cause disruptions.[23] It can affect factor markets,[24] such as those for raw materials and labor.[25] These disruptions spread impacts to linked firms,[26] propagating upstream and downstream via supply chain linkages.[27] These firms face challenges such as carbon lock-in and green premiums.[28] Carbon lock-in refers to path-dependent technological and institutional reliance on fossil fuels,[29] and its transition costs are prohibitive.[30] The phaseout of high-carbon facilities and technologies leads to idle assets and capital waste.[31] Meanwhile, as low-carbon technologies are deployed, associated cost increases are passed through supply chains, contributing to rising prices across sectors.[32] Rising production costs may trigger inflation.[33] This will trigger global supply chain instability,[34] with disturbances spreading across supply chain networks to impair firm operations and economic development.[35]

This paper conceptualizes carbon reduction risks as exogenous disruptive forces. These forces arise from the mismatch between the pace of the decarbonization transition and the adaptive capacity of economic and industrial systems, materializing through systemic frictions, cost distortions, and structural rigidities across production and supply networks. Such shocks can disrupt the steady-state operation of supply chain networks by amplifying vulnerabilities across inter-firm linkages. Consequently, investigating the resilience of supply chain networks to withstand and recover from these external perturbations is of paramount theoretical and empirical significance for maintaining industrial continuity and sustainable development.

The manufacturing supply chains exhibit complex network characteristics.[36] Driven by economic globalization and the rise of the network economy, this complexity has become increasingly prominent. Risk propagation is inherently a dynamic process, jointly shaped by the initial characteristics of risks and the underlying network structure. Thus, exploring risk propagation from a complex network perspective aligns more closely with real-world scenarios. External risk disturbances can cause node or link failures.[37] These failures propagate through interconnected nodes[38] and trigger cascading systemic collapses,[39] thereby driving risk propagation.[40] Existing research on these mechanisms has focused on three core areas: identifying vulnerable links and critical nodes in supply chain

networks,[41] analyzing patterns and quantitative measures of risk propagation intensity,[42] and examining transmission pathways and mitigation strategies.[43] Drawing on complex network theory, scholars have also explored the formation of supply chain networks, information flow channels, and inherent risk dynamics,[44] establishing a robust theoretical foundation for studying industrial network interactions.[45]

Scholars have extensively examined carbon reduction risks in manufacturing[46] and the mechanisms by which supply chain risks are transmitted.[47] These studies clarify that carbon reduction risks propagate through supply chain networks and induce cascading effects, and elaborate on their specific manifestations, including the dual pressures faced by developing economies, the emergence of the low-carbon poverty paradox, and practical dilemmas such as carbon lock-in and green premiums. In addition, relevant scholars have adopted complex network methods to identify risks in supply chain networks, analyze their transmission patterns, and explore sector-specific risk transmission paths and corresponding mitigation strategies, which provide important methodological references for this paper. Despite these advances, gaps still exist in the literature. Most studies focused on impacts on raw material prices,[48] conventional firm operations, or international trade.[49] Research on the propagation of carbon reduction risks within supply chain networks remains relatively limited.[50]

Unlike previous research, which often overlooks supply chain network-based risk propagation or lacks targeted analysis of these dynamics, this study conducted a data-driven investigation into the propagation of carbon reduction risks within supply chain networks. Drawing on an interdisciplinary framework that integrates economics and complex network theory, this study developed a theoretical economic model and conducted numerical simulations to examine how carbon reduction risks in the manufacturing sector propagate through supply chain networks. The mechanism of how carbon reduction risks in the manufacturing sector propagate through supply chain networks was decomposed into two layers: the micro-level mechanism of carbon reduction risk shocks acting on focal firms in the supply chain, and the macro-level mechanism of focal firms transmitting such shocks to their upstream and downstream counterparts from the perspective of the topological structure of the overall supply chain network. It leveraged a complex network model and a multi-stage supply chain benchmark model for this analysis and further conducted a multidimensional measurement of risk-shock transmission in the supply chain network, comprehensively capturing the total propagation rounds and the operational efficiency of the supply chain network. It not only addresses the gap in the literature on network-centric carbon reduction risk transmission but also clarifies the complex network characteristics of supply chains. This study provides actionable insights for practitioners and policymakers on balancing decarbonization goals with supply chain stability.

To guide this investigation, the following research questions are posed:

(i) What are the key determinants of firm positioning within multi-stage supply chain networks, and how do pricing strategies, production costs, transportation expenditures, and carbon reduction investment expenditures shape such positioning?
(ii) What is the cascading transmission path of carbon reduction risks in supply chain networks, and how do these risks trigger bidirectional propagation between upstream and downstream segments?
(iii) How do different supply chain network structures differ in robustness against random shocks and targeted attacks, and how does the share of shocked nodes affect the efficiency of these networks? Specifically, how do the operational endurance, cumulative effective functionality, and efficiency degradation trajectory of different network structures differ under the two attack modes, even with similar average decline rates (ADRs)?
(iv) What is the relationship between the firm's strategic resilience parameter (β), external dependency parameter (γ), and the failure probability of supply chain networks, and do parameter adjustments exert heterogeneous resilience effects across different network structures? Specifically, how do the interaction effects of β and γ influence the resilience of different network structures under distinct attack regimes, and whether moderate parameter values yield optimal resilience while excessive values accelerate network failure?

2. Mechanism of risk propagation

The resilience of supply chain networks refers to their capacity to maintain core operational functions, resist risk diffusion, mitigate functional decay, and adapt structurally and operationally in response to evolving risks under uncertainty. It encapsulates the supply chain network's ability to resist, buffer, and adapt throughout the risk-impact period, highlighting the sustained operational effectiveness of the network. This concept integrates system stability, anti-fragility, and dynamic adaptability, which are central to understanding how supply chains endure and recover from disruptions.

In the context of this study, supply chain network

resilience manifests specifically during the propagation of carbon reduction risks through supply chain networks. It reflects the supply chain network's ability—leveraging its topological characteristics (e.g., random, small-world, or scale-free structures—to withstand further risk transmission, slow the decline in the proportion of functional nodes, delay the onset of critical failure thresholds, reduce the amplitude of abrupt fluctuations, and continuously maintain a sufficient level of operational nodes. This ensures that the supply chain retains its basic operational functionality despite carbon reduction risk shocks, thereby preventing a rapid collapse in network efficiency due to the propagation of carbon reduction risks.

The supply chain network possesses the fundamental characteristics of a network, comprising multiple suppliers, manufacturers, distributors, and customers.[51] A graphical overview of the supply chain network structure is given in Figure 1. As illustrated, the supply chain network exhibits a multi-tiered and interconnected topology. Specifically, the upstream tier consists of a pool of suppliers that establish many-to-many sourcing relationships with manufacturers in the production tier. These manufacturers distribute goods to multiple distributors, and the distribution tier ultimately connects to downstream customers. This connectivity defines the structural complexity and resilience of the supply chain network.

The supply chain network encompasses both single-chain production activities and cross-chain collaborative development.[52] Drawing on complex network theory, we formalized the supply chain network as $G(C, E, V^C, V^D)$, where $C=\{a_u \mid u=1,2,3\ldots, N\}$ denotes the node set comprising all firms in the supply chain network. Nodes represent distinct entities across the supply chain hierarchy, such as raw material suppliers, component manufacturers, final assemblers, distributors, retailers, and end customers. $E=\{M_{uv} \mid u,v=1,2,3\ldots,N\}$ represents the edge set that characterizes the business relationships between paired nodes a_u and a_v. A binary indicator is adopted: if $M_{uv}=1$, it indicates that there are realistic connections between nodes a_u and a_v, such as information transmission, product flow, and economic transactions; conversely, if $M_{uv}=0$, it indicates the absence of such practical interactions between firm nodes. $V^C=\{a_u^c \mid u=1,2,3,\ldots,N\}$ denotes the role attribute set of node firms, where a_u^c explicitly identifies the functional role of the node a_u in the supply chain network. $V^D=\{V_{uv}^D \mid u,v=1,2,3,\ldots,N\}$ denotes the edge weight set, with V_{uv}^D quantifying the strength of the relationship between the origin node a_u and destination node a_v. Weight values are determined by the connection degree of the origin node in the supply chain network,[53] and their practical manifestations include transaction volume, frequency of business interactions, or the degree of technological dependency between firms. A higher V_{uv}^D value indicates a stronger resource dependency of the firm on its counterpart. This metric quantitatively characterizes the asymmetric interdependence patterns within manufacturing supply chains,[54] in which nodes with

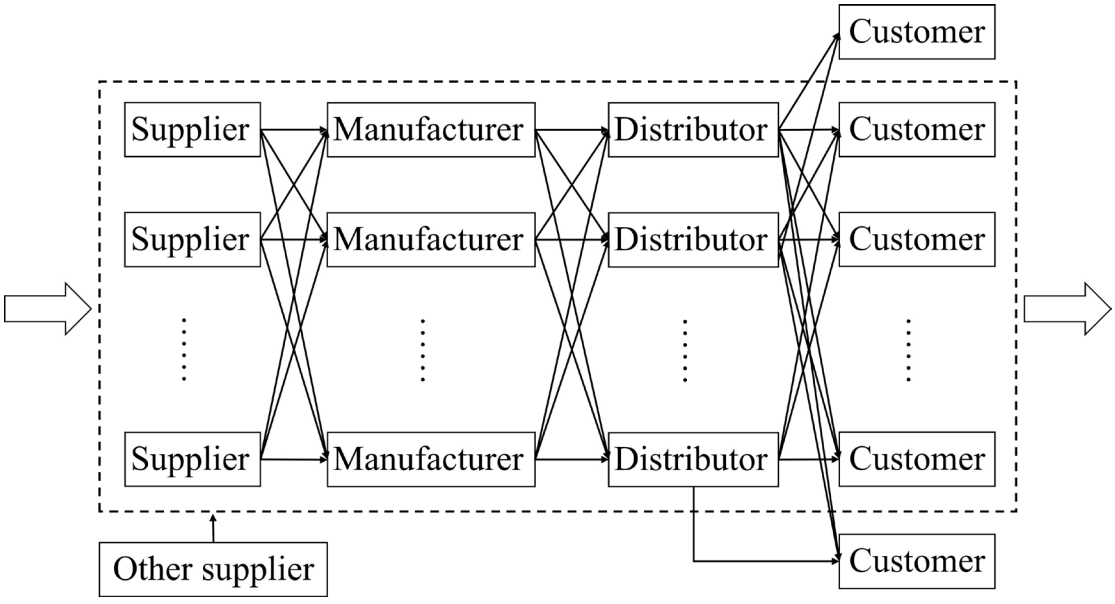

Figure 1. The structure of supply chain networks

higher degree centrality exert more significant influence on risk propagation dynamics.

Drawing on the benchmark model of multi-stage production fragmentation,[55] $j \in \{1,2,\ldots,J\}$ denotes the various stages in a supply chain network within the multi-stage division of labor. Values ranging from 1 to *J* represent the upstream and downstream stages of the supply chain. Given that the production process in a supply chain network involves multiple stages and the use of intermediate products, the Cobb–Douglas production function was employed for theoretical derivation to simplify the solution of the general equilibrium. Based on the Cobb–Douglas production function, the production function of firm *i* in stage *j* of the supply chain network is as follows:

$$f_i^j = Z_i^j[(X_i^j)^{1-\alpha_i}\left(L_i^j\right)^{\alpha_i}]^{\theta^j}(M_i^{j-1})^{1-\theta^j} \quad (1)$$

where f_i^j denotes the production output level of firm i at stage j in the supply chain network, Z_i^j denotes the production technology level of firm i at stage j in the supply chain network, the variable X_i^j denotes the energy input of firm i, L_i^j denotes the labor input of the firm, M_i^{j-1} denotes the intermediate products of the firm, α_i denotes the output share of labor input, $1-\alpha_i$ denotes the output share of carbon reduction input, θ^j denotes the value-added share of production factors used in the current stage of production, and $1-\theta^j$ denotes the cumulative value-added share of intermediate products from stage $j-1$ employed in the production process.

To streamline the pricing framework and elucidate the cost-transmission mechanism while controlling for confounding variables, the assumption of a perfectly competitive market was employed. This methodological choice allows for a clear revelation of the general equilibrium relationships across various stages of the supply chain network.

Starting from the production function given in **Equation 1**, we first formulated the cost minimization problem with the objective function:

$$c_i = P_i X_i + w_i L_i \quad (2)$$

where P_i denotes the unit price of energy input X_i, and w_i denotes the wage rate (i.e., the unit price of labor input L_i). We then constructed the Lagrangian by incorporating the production function as a constraint. Taking the first-order partial derivatives of the Lagrangian with respect to X_i and L_i and setting them equal to zero yielded two first-order conditions. Solving these conditions simultaneously gave the optimal relationship between the two inputs—specifically, an expression for X_i as a function of L_i. Substituting this relationship back into the production function yielded the conditional factor demand functions for both inputs. Finally, substituting these conditional factor demand functions into the original cost function yielded the unit cost function presented in **Equation 3**.

$$c_i = \left(\frac{P_i}{1-\alpha_i}\right)^{1-\alpha_i}\left(\frac{w_i}{\alpha_i}\right)^{\alpha_i} \quad (3)$$

As shown in **Equation 3**, the unit energy input price P_i and labor wage w_i jointly determine firms' production costs. This interdependent relationship implies that fluctuations in market pricing mechanisms and labor remuneration jointly shape the cost structure of manufacturing production. Transportation costs arise in the shipment process. Assuming that firm *n* sources inputs from firm *i*, firm *i* must ship at least $\tau_{in} \geq 1$ units of product to deliver one usable unit to firm *n* to compensate for transportation losses and satisfy the required supply quantity. Thus, based on the general equilibrium conditions, the price of the products produced by firm *i* at stage *j* in the supply chain network can be derived as follows:

$$p_{l(j)}^j = \frac{c_{l(j)}^{\theta j-1}(p_{l(j-1)}^{j-1}\tau_{l(j-1)l(j)})^{1-\theta j}}{z_{l(j)}^j} \quad (4)$$

In **Equation 4**, $i = l(j)$, $j \in \{1,2,\cdots,J\}$ denotes the embeddedness of firm *i* at the *j*-th stage within a specific supply chain. This parameter quantifies the degree of integration and positional significance of the firm in the hierarchical structure of the supply chain network. $c_{l(j)}^{j-1}$ denotes the cost incurred at stage $j-1$ for production at stage *j*. $\tau_{l(j-1)l(j)}$ denotes the transportation cost between stage $j-1$ and stage *j*. $p_{l(j-1)}^{j-1}$ indicates that the product price at stage $j-1$ affects the unit energy input price at stage *j*, while the price at stage $j-1$ is, in turn, determined by that at stage $j-2$. This interdependency generates a sequential chain effect that propagates upstream along the supply chain until it reaches the initial production node.

Drawing on the study of Antràs and Gortari,[55] we defined:

$$\varepsilon_i^j[s] = E_j\left[\left(p_{l(j)}^j \tau_{l(j)i}\right)^s\right] \quad (5)$$

from which the probability that firm *i* supplies products to firms in stage $j+1$ from stage *j* can be derived.

$$Pr(l(j)=i) = \frac{A_i\left(\left(c_i^j\right)^{\theta^j}\tau_{l(j-1)i}\right)^{-\varphi\beta^j}\varepsilon_i^{j-1}[(1-\theta^{j+1})(1-\theta^j)]^{-\varphi\beta^{j+1}}}{\sum_{n\in N}A_n\left(\left(c_n^j\right)^{\theta^j}\tau_{l(j-1)n}\right)^{-\varphi\beta^j}\varepsilon_n^{j-1}[(1-\theta^{j+1})(1-\theta^j)]^{-\varphi\beta^{j+1}}} \quad (6)$$

The numerator in **Equation 6** reflects the competitive

advantage of firm i in the overall market competition. The unit energy input price affects the firm's competitive advantage, which in turn influences the probability that firm i supplies products to downstream manufacturers, thereby affecting the volume of products available at stage $j+1$.

As shown in **Equations 3, 4, and 6**, factors such as a firm's product pricing, production costs, transportation costs, and carbon reduction costs all affect the embedding probability at stage j of the supply chain. Therefore, the quantity of products that firm i supplies from stage j to stage $j+1$ firms can be determined based on the embedding probability and the market capacity q_{j+1} in stage $j+1$.

$$Q_{j+1} = \Pr\left(l(j) = i\right) q_{j+1} \tag{7}$$

Figure 2 illustrates the risk propagation mechanism within supply chain networks under carbon reduction risk shocks in the manufacturing industry, using a flowchart to visualize the dynamic transmission process. This diagram depicts the causal relationships and feedback loops associated with carbon reduction risks. The analysis captures how such risks propagate across interconnected nodes within manufacturing ecosystems.[56] Specifically, the framework examines three critical nodal components: material suppliers, production facilities, and distribution networks. The graphical model demonstrates the risk-transmission pathways through which environmental effects disseminate among these operational units. Furthermore, it visualizes recursive interactions in which carbon reduction outcomes may reinforce systemic vulnerabilities across the supply chain.[57] To simplify the analysis, this study focuses on trade interactions between firm A and its upstream or downstream partners at stage *j*. Firm A supplies products to firms B, C, and D in the $j+1$ stage, while firms E, F, and G in the $j-1$ stage provide products to firm A in the *j* stage. We assumed that the carbon reduction risks in the manufacturing industry affect the supply chain network by acting on firm A at stage *j*, and propagate through the upstream and downstream linkages within the supply chain to affect firms B, C, and D at stage $j+1$ and firms E, F, and G at stage $j-1$.

The probabilities that firm A supplies products to firms B, C, and D in the $j+1$ stage are $\Pr\left(l(j) = A \mid B\right)$, $\Pr\left(l(j) = A \mid C\right)$, and $\Pr\left(l(j) = A \mid D\right)$, respectively. From **Equation 7**, the quantities of products provided by firm A

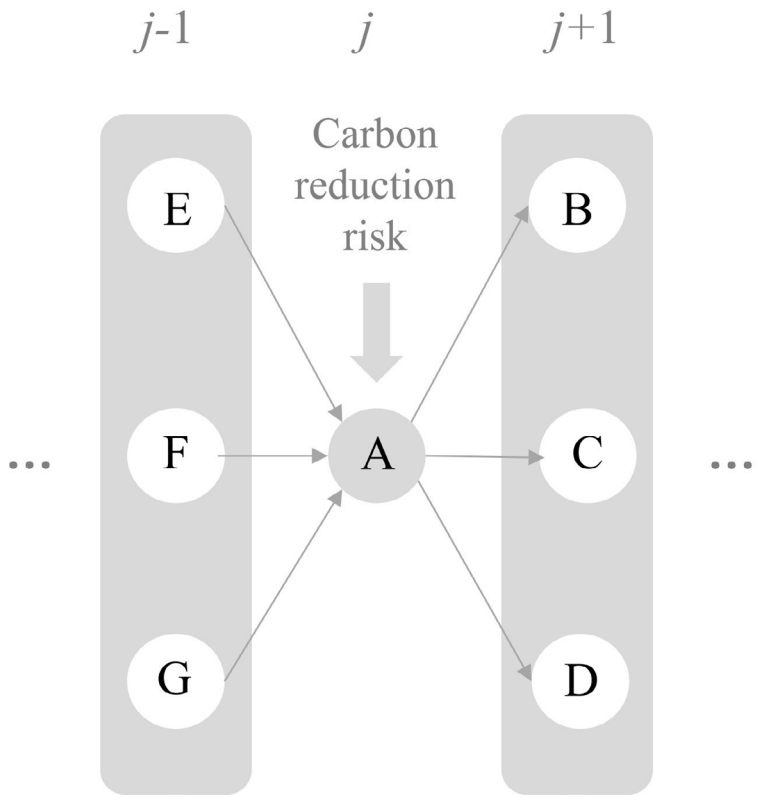

Figure 2. Risk propagation mechanism diagram

to firms B, C, and D in the $j+1$ stage are respectively:

$$\begin{aligned} Q_{j+1}A \mid B &= \Pr\left(l(j)=A \mid B\right)q_{j+1}(B) \\ Q_{j+1}A \mid C &= \Pr\left(l(j)=A \mid C\right)q_{j+1}(C) \\ Q_{j+1}A \mid D &= \Pr\left(l(j)=A \mid D\right)q_{j+1}(D) \end{aligned} \tag{8}$$

Thus, the total quantity of products provided by firm A to the firms in stage $j+1$ is:

$$Q_{j+1}s = \sum_{s\in B,C\ D} \Pr\left(l(j)=A \mid s\right)q_{j+1}(s) \tag{9}$$

After firm A is subjected to carbon reduction risk shocks, the probability of firm A supplying products to firms B, C, and D in stage $j+1$ becomes $\Pr\left(l(j)=A \mid B\right)'$, $\Pr\left(l(j)=A \mid C\right)'$ and $\Pr\left(l(j)=A \mid D\right)'$. After being impacted by exogenous risks, the quantity of products that firm A supplies to firms B, C, and D in the $j+1$ stage becomes:

$$\begin{aligned} Q_{j+1}A \mid B' &= \Pr\left(l(j)=A \mid B\right)'q_{j+1}(B) \\ Q_{j+1}A \mid C' &= \Pr\left(l(j)=A \mid C\right)'q_{j+1}(C) \\ Q_{j+1}A \mid D' &= \Pr\left(l(j)=A \mid D\right)'q_{j+1}(D) \end{aligned} \tag{10}$$

Under the influence of carbon reduction risks, the total amount of products provided by firm A to firms in stage $j+1$ becomes:

$$Q_{j+1}s' = \sum_{s\in B,C,D} \Pr\left(l(j)=A \mid s\right)'q_{j+1}(s) \tag{11}$$

Similarly, the probabilities that firms E, F, and G in stage j-1 supply products to firm A in stage j are $\Pr\left(l(j\text{-}1)=E \mid A\right)$, $\Pr\left(l(j\text{-}1)=F \mid A\right)$, and $\Pr\left(l(j\text{-}1)=G \mid A\right)$, respectively. The quantity of products that firms E, F, and G supply to firm A becomes:

$$\begin{aligned} Q_jE \mid A &= \Pr\left(l(j-1)=E \mid A\right)q_j(A) \\ Q_jF \mid A &= \Pr\left(l(j-1)=F \mid A\right)q_j(A) \\ Q_jG \mid A &= \Pr\left(l(j-1)=G \mid A\right)q_j(A) \end{aligned} \tag{12}$$

The total amount of products provided by firms E, F, and G to firm A becomes:

$$Q_jT = \sum_{T\in E,F,G} \Pr\left(l(j-1)=T \mid A\right)q_j(A) \tag{13}$$

Following the impact of carbon reduction risk in the manufacturing industry, firm A is significantly affected. The quantity of products supplied by firm A to stage $j+1$ firms changes, which in turn alters firm A's demand for products from stage j-1 firms. Consequently, the market capacity at stage *j* shifts from $q_j(A)$ to $q_j(A)'$. The quantity of products supplied by firms E, F, and G to firm A becomes:

$$\begin{aligned} Q_jE \mid A' &= \Pr\left(l(j-1)=E \mid A\right)q_j(A)' \\ Q_jF \mid A' &= \Pr\left(l(j-1)=F \mid A\right)q_j(A)' \\ Q_jG \mid A' &= \Pr\left(l(j-1)=G \mid A\right)q_j(A)' \end{aligned} \tag{14}$$

Under the influence of carbon reduction risk, the total amount of products provided by firms E, F, and G to firm A becomes:

$$Q_jT' = \sum_{T\in E,F,G} \Pr\left(l(j-1)=T \mid A\right)q_j(A)' \tag{15}$$

In summary, carbon reduction risks raise firms' unit product costs, which, in turn, drive up product prices.[58] This leads to a reduction in product supplies to downstream buyers, and the supply contraction further lowers the procurement demand of the affected firms. For upstream firms, a decline in downstream supply can also result in product inventory accumulation at the current stage, thereby increasing the risk of overload failure. Ultimately, this gives rise to the bidirectional transmission of risks both upstream and downstream along the supply chain. It is evident that carbon reduction risks in the manufacturing sector undermine the stability of the entire supply chain.

3. Risk propagation simulation

3.1. Parameter settings

3.1.1. Initial load

The initial load (L_r^0) refers to the resource stock held by a node firm at the initial stage of supply chain network formation. It is determined by the firm's organizational characteristics and is influenced by its node degree and the number of upstream and downstream partners. In supply chain network analysis, a firm (node) with a higher degree maintains more connections with other nodes. Such greater connectivity indicates more complex interdependencies within the network structure. This topological complexity increases the node's exposure to potential systemic risks and vulnerability propagation. Accordingly, highly connected nodes face elevated threat levels due to their critical role in risk transmission pathways. The initial load (L_r^0) comprises the initial demand load (L_r^D) and initial supply load (L_r^S), which are defined as follows:

$$L_r^0 = \left(k_r \sum_{l\in\varphi_r^{in}\cup\varphi_r^{out}} k_l\right)^{\alpha}, r=1,2,3,\ldots,N \tag{16}$$

$$L_r^D = \left(k_r^{in} \sum_{l\in\varphi_r^{in}\cup\varphi_r^{out}} k_l\right)^{\alpha}, r=1,2,3,\ldots,N \tag{17}$$

$$L_r^S = \left(k_r^{out} \sum_{l\in\varphi_r^{in}\cup\varphi_r^{out}} k_l\right)^{\alpha}, r=1,2,3,\ldots,N \tag{18}$$

Let N denote the total number of nodes in the supply chain network. φ_r^{in} denotes the set of upstream nodes of firm r, while φ_r^{out} denotes the set of downstream nodes of firm r. k_r indicates the degree of the nodes at both ends of the edge, including both the in-degree k_r^{in} and out-degree k_r^{out} values. k_l denotes the sum of the degrees of all upstream and downstream nodes. α is the parameter that regulates the distribution of node loads in the network. The value of α affects the initial load of the nodes. A smaller α implies a more uniform initial load distribution among the nodes, thereby enhancing the supply chain network's ability to resist external risks.

3.1.2. Node capacity boundary

Nodes in the supply chain network have a capacity boundary, defined as the maximum load that each node can bear.[59] This upper limit represents the maximum operational load a node firm can manage and reflects its inventory-handling capability.[60] When the load transmitted to the focal firm node from various directions within the supply chain network exceeds its upper capacity limit, the node will suffer from overload failure.[61] Overload failure tends to occur in upstream node firms. When downstream firms are exposed to external risk disturbances, upstream firms are more likely to face overload failure due to inventory accumulation. Therefore, this paper assumes that the upper capacity limit of nodes (L_r^{max}) in the supply chain network is proportional to the initial supply load of the node.

$$L_r^{\max} = (1+\beta) L_r^S, 0 < \beta < 1 \tag{19}$$

where β denotes the strategic resilience parameter, which quantifies a firm's dynamic capability to absorb overload shocks in the supply chain network. In practical operational terms, β is directly linked to three core measurable metrics. First is the ratio of safety stock to average inventory, which reflects the level of inventory redundancy a firm maintains. Second is the percentage of critical materials sourced from multiple vendors, a metric that captures the degree of multi-sourcing implementation. Third is the speed of production line reconfiguration, which measures the extent of flexible production capacity. A higher value of β indicates that a firm has invested more heavily in these tangible resilience-building levers. As a result, the firm faces a lower probability of node failure when encountering downstream demand disruptions or inventory accumulation risks. The constraint $0 < \beta < 1$ is set based on a practical economic trade-off: the marginal cost of enhancing resilience through additional inventory, multi-sourcing, or flexible production increases as β rises, and firms will not pursue infinite resilience due to cost-efficiency considerations.

The lower bound of node capacity refers to the minimum load required for each node to maintain normal operation, corresponding to the minimum demand for a node to achieve a break-even state.[62] When the load transmitted to a node firm from all directions within the supply chain network is insufficient to meet the node's minimum required capacity, the node fails due to underloading. Underload failure typically occurs in downstream node firms. When upstream firms are exposed to external risk disturbances, downstream firms are prone to underload failure due to insufficient raw material supply. This paper assumes that the lower bound of node capacity (L_r^{min}) in the supply chain network is inversely proportional to the initial demand load of the node.

$$L_r^{\min} = \gamma L_r^D, 0 < \gamma < 1 \tag{20}$$

where γ represents the external dependency parameter, which gauges a firm's vulnerability to underload shocks triggered by upstream supply disruptions. From an operational measurement perspective, γ can be calibrated using two key quantitative indicators. The first indicator is the share of procurement value from the single largest supplier, which reflects the degree of supplier concentration. The second indicator is the percentage of key inputs sourced from a single geographic region, which measures the level of geographic concentration in supply. A higher value of γ implies that a firm relies more heavily on specific upstream partners or a single supply region for its core inputs. This high level of operational reliance elevates the risk of raw material shortages, thereby increasing the probability of node failure when the firm is exposed to upstream supply shocks. The range $0 < \gamma < 1$ aligns with real-world supply chain structures: complete diversification of suppliers (γ approaches 0) is often not feasible due to high coordination costs and economies of scale in procurement, while full reliance on a single source (γ equals 1) is extremely rare in practice due to obvious risk exposure.

3.1.3. Node load redistribution

When a node failure occurs in a supply chain network due to targeted attacks, upstream and downstream firms will actively seek alternative nodes with comparable resource capabilities.[63] This strategic adaptation enables either the reinforcement of existing partnerships or the formation of new collaborative alliances within the supply chain network. Such relationship restructuring helps mitigate operational load losses caused by the failed node, thereby sustaining supply chain network functionality via resource redistribution.[64] This adaptive reconfiguration mechanism

reflects the supply chain network's resilience in maintaining operational continuity while redistributing carbon reduction responsibilities across alternative pathways. The load redistribution process is implemented as follows:

$$\Delta L_{yr} = L_r \frac{k_y^{\alpha}}{\sum_{n \in \sigma_r} k_n^{\alpha}} \tag{21}$$

Let ΔL_{yr} denote the load allocated from node y to its adjacent node r following the paralysis of a node. σ_r denotes the set of all nodes adjacent to node r. Following the failure of node r, its supply load will be redistributed to node e within the same operational phase that shares comparable supply resource characteristics. This redistribution mechanism elevates the supply load borne by node e. In the meantime, the failure of node r will lead to a lack of suppliers for downstream node y, thereby causing a decline in the demand load of the downstream nodes. The reallocation of supply and demand loads is represented as follows:

$$L_e^{S'} = L_y^{S'} + L_r^{S'} \frac{k_e^{out}}{\sum_{n \in \sigma_r} k_n^{out}} \tag{22}$$

$$L_y^{D'} = L_y^{D'} - L_r^{D'} \frac{k_y^{in}}{\sum_{n \in \sigma_r} k_n^{in}} \tag{23}$$

$L_e^{S'}$ denotes the supply load quantity received by node e under its own supply load condition after undergoing supply load redistribution from node r. $L_y^{D'}$ denotes the demand load quantity at node y under its inherent demand load status following the demand load redistribution at node r.

3.1.4. Node failure determination

Following the failure of adjacent nodes and the subsequent redistribution of their loads, the loads borne by surviving nodes must remain within their respective effective load boundaries.[65] Otherwise, cascading failures may arise. During load redistribution, a node will fail if its effective load capacity falls below its minimum capacity threshold or exceeds its maximum tolerable capacity limit. This failure mechanism reflects the dual constraints imposed on supply chain network nodes: lower-bound stability maintenance and upper-bound overload tolerance. The load capacity received by upstream node firms from failed nodes is expressed as follows:

$$L^{t+1} = L^t + \Delta L^{t+1} \tag{24}$$

If the load capacity remains within its tolerable threshold after redistribution by $L^{min} < L^{t+1} < L^{max}$, then the node can maintain normal operation within the supply chain network. If either $L^{t+1} < L^{min}$ or $L^{t+1} > L^{max}$ occurs, the redistributed load capacity will exceed its load-bearing capacity threshold, thereby causing the further propagation of cascading failures.

The load capacity received by downstream node firms from failed nodes is denoted as:

$$L^{*t+1} = L^{*t} - \Delta L^{*t+1} \tag{25}$$

If $L^{*min} < L^{*t+1} < L^{*max}$ is satisfied, the node can maintain normal operation within the supply chain network. However, if $L^{*t+1} < L^{*min}$ or $L^{*t+1} > L^{*max}$ occurs, the node will also fail, thereby causing cascading failures to propagate further.

Figure 3 illustrates the evolutionary process of cascade failure. In the initial state, supply chain networks maintain a stable operational state. Nodes possess a certain capacity to resist external risks, enabling them to sustain normal operations when confronted with external risk shocks. Upon experiencing external carbon reduction risk shocks, these shocks first target and disable partial nodes within the supply chain network. Nodes impacted by the shocks transmit the risk to their adjacent upstream and downstream firms. These neighboring nodes then propagate the risk to their own adjacent nodes, thereby spreading the risk across the entire supply chain network. It proceeds to the node failure determination stage, where the scale of failed nodes is assessed. The process terminates only when no further nodes fail; otherwise, the system reallocates loads and repeats the cycle until the termination condition is satisfied.

3.1.5. Measurement of supply chain network efficiency

To evaluate the impact of carbon reduction risks on supply chain networks in the manufacturing sector, this study introduced a robustness assessment framework.[66] Specifically, supply chain network efficiency is adopted as a key performance metric. This metric is defined as the ratio of functional nodes to the original scale of the supply chain network under disruption scenarios. Its mathematical formulation is expressed as follows:

$$E = \frac{N^*}{N} \tag{26}$$

where E denotes the supply chain network efficiency, N^* denotes the number of nodes that remain functional within the supply chain network after being subjected to carbon reduction risk shocks, and N denotes the number of nodes in the initial supply chain network that are not exposed

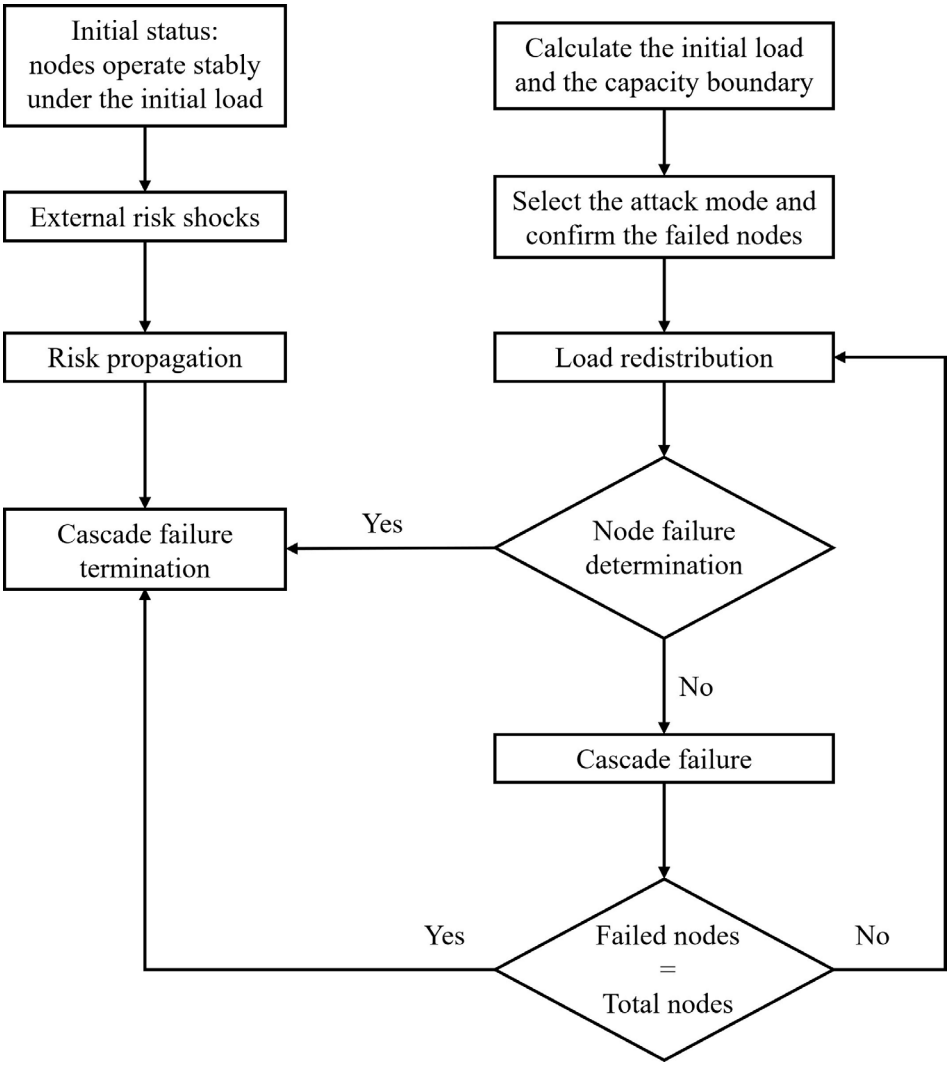

Figure 3. Cascade failure evolution process

to carbon reduction risk shocks. This metric quantifies the system's survivability by measuring its capacity to maintain structural and functional integrity as carbon reduction risks propagate. The higher the proportion of non-failed nodes, the smaller the impact of external carbon reduction risks on the supply chain network.[67] This indicates a stronger overall supply chain network resilience and better anti-destruction performance.

3.1.6. Measurement of supply chain network resilience

Based on the aforementioned research on measuring supply chain network efficiency, we could dynamically track the efficiency of supply chain networks under carbon reduction risk shocks. However, relying solely on supply chain network efficiency curves may overlook the actual trajectory of operational performance degradation between the onset of a risk shock and eventual network collapse. One supply chain network might fail only at a late stage, but its operational capacity could have deteriorated significantly well before that point. In contrast, another supply chain network might ultimately collapse, but maintain relatively high operational efficiency until just prior to failure. Clearly, the latter holds substantially greater practical business value. However, such a distinction remains difficult to capture using conventional supply chain network efficiency metrics alone. To fundamentally address this limitation, this paper proposes a comprehensive, multidimensional measurement framework designed to precisely quantify the full performance degradation trajectory. This framework

comprises four indicators:

(i) Indicator 1: Threshold round of 50% efficiency (T50). This indicator focuses on the critical turning point at which the supply chain network transitions from effective operation to semi-paralysis as carbon reduction risks propagate through the network. By setting an efficiency threshold, it captures the risk transmission round in which the proportion of effective nodes first falls below 50% of the initial value, reflecting the phased resilience baseline of the supply chain network against carbon reduction risks. We extracted the time series of the proportion of effective nodes at each round of carbon reduction risk propagation. The set of time series of the proportion of effective nodes was denoted as $E = \{e_1, e_2, \cdots, e_n\}$, where e_1 corresponds to the initial proportion of effective nodes. We then computed the 50% degradation threshold as:

$$T_{50} = 0.5e_1 \tag{27}$$

Next, we scanned the sequence E to identify the earliest round $i, i \in \{1, 2, \cdots, n\}$ such that $e_i \le T_{50}$. If $e_i \le T_{50}$, this round was defined as T_{50}. If the series never fell below this threshold during the entire simulation, the case was labeled as threshold not breached.

(ii) Indicator 2: Area under the effective node ratio curve (AUC). This indicator quantifies the overall resilience of the supply chain network throughout the entire process of carbon reduction risk transmission. By calculating the area enclosed by the time-series curve of the effective node proportion and the horizontal axis, it integrates dual information on transmission round length and effective proportion per round. A larger area indicates stronger overall resilience.

(iii) Indicator 3: Total effective value (TEV). This indicator focuses on the practical operational stage of the supply chain under carbon reduction risk impacts. It counts only rounds in which the proportion of effective nodes is ≥50% of the initial value. By summing these values, it quantifies the cumulative value of effective operation, reflecting the actual available resilience level of the supply chain network. A larger TEV value indicates stronger overall resilience.

(iv) Indicator 4: ADR. This indicator quantifies the overall decline rate in the effective operational capacity of the supply chain network during carbon reduction risk transmission, reflecting the stability of the network in resisting such risks. A smaller ADR indicates stronger risk resistance and stability, and provides decision-makers with more intervention time.

3.2. Cascading risk propagation simulation

3.2.1. Risk propagation under different network structures

Real-world supply chain networks often exhibit structural characteristics consistent with those of complex network models. Empirical and theoretical studies suggest that their topologies can generally be categorized into three canonical types: scale-free, random, and small-world networks.[68] To systematically investigate the propagation dynamics of carbon reduction risk within supply chain networks, this study conducted simulations and analyses for each of the three network structures. Using Python 3.8, we generated three types of networks.[69] The parameters were set as α = 0.8, β = 0.3, and γ = 0.7. Twenty nodes were randomly selected as the initial failure nodes under random attack conditions. In contrast, the 20 nodes with the highest degree centralities in the supply chain network were designated as targets for targeted attacks.

Figure 4 illustrates the evolution of supply chain network efficiency under random and targeted attacks across three distinct network structures. The x-axis represents the order of risk propagation, while the y-axis denotes the proportion of effective nodes. The figure depicts the efficiency dynamics of scale-free, random, and small-world networks under external carbon reduction risk shocks.

The results reveal that the speed and patterns of risk propagation exhibit significant heterogeneity across the three distinct network structures.[70] When the supply chain network was exposed to random shocks, the random network displayed strong robustness and could withstand risks associated with stochastic disturbances. In contrast, the scale-free network showed moderate robustness, whereas the supply chain network collapsed rapidly after three rounds of risk propagation. The small-world network possessed the weakest risk resistance; it gradually collapsed once exposed to random shocks.

Under targeted attacks, small-world networks exhibited the greatest risk resistance, with some nodes remaining functional even after multiple rounds of risk propagation. Random networks ranked second in robustness, maintaining relatively high resilience in the early stages of targeted attacks, although their efficiency declined sharply as the number of risk-propagation rounds increased. Scale-free networks displayed the weakest robustness, as targeted attacks led to rapid network collapse.

The targeted attack strategy primarily targets high-degree nodes within a supply chain network.[71] This

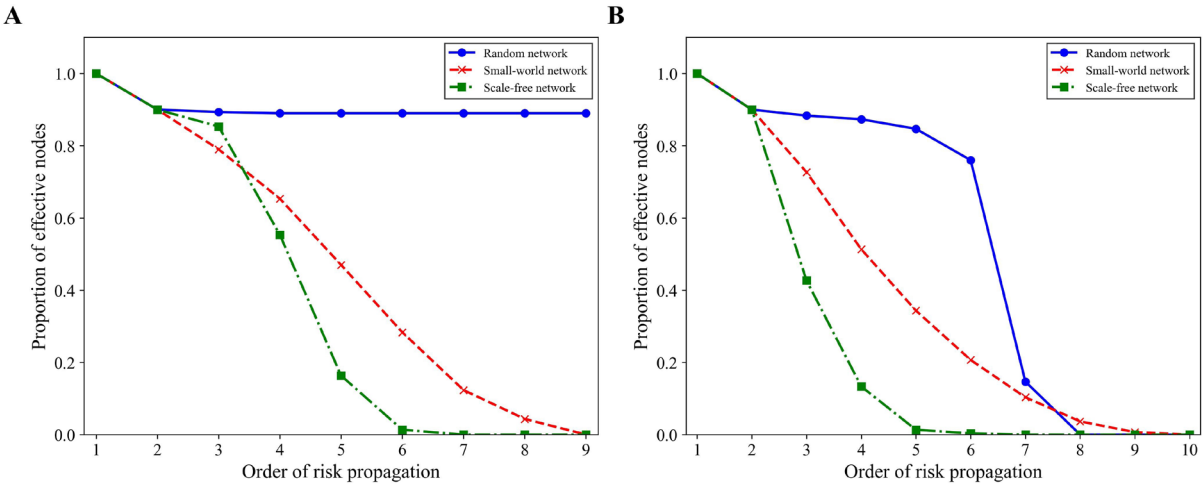

Figure 4. Network efficiency under (A) random attack and (B) targeted attack on different network structures

selective node removal disrupts a large number of adjacent connections, since each targeted node maintains numerous neighboring edges. Consequently, the cumulative edge breakdown impairs network connectivity. Such structural deterioration triggers rapid system-wide collapse via cascading failure mechanisms. Therefore, all three network types are vulnerable to targeted attacks.[72]

Table 1 presents the measured values of the four resilience indicators for the three canonical network structures under both random and targeted attacks. As shown in Table 1, distinct resilience patterns emerged across different network structures under random versus targeted attacks. Under random attacks, the random network demonstrated the strongest overall resilience: its T_{50} threshold was never breached, and it achieved the highest AUC (7.1883) and TEV (8.1333) among all three network types, indicating sustained high operational effectiveness throughout the risk-propagation process. In contrast, although the scale-free network also reached its T_{50} at round 5, its substantially lower AUC (2.9833) and TEV (3.3067) revealed a more rapid decay in effective functionality. Under the more damaging targeted attacks, all networks degraded earlier and faster, with the scale-free network performing worst—reaching T_{50} as early as round 3 and recording the lowest AUC (1.9767) and TEV (1.9000)—highlighting its vulnerability due to its dependence on critical hubs. The random network, while eventually falling below the threshold at round 7, still maintained significantly higher AUC (4.9100) and TEV (5.2633) than the other two structures, underscoring its superior robustness. Notably, the ADR values were consistently either 0.1000 or 0.1111 across all scenarios, suggesting similar average rates of decline. However, when considered alongside T_{50}, AUC, and TEV, it becomes clear that comparable decay rates do not imply equivalent operational endurance or cumulative value. This discrepancy reinforces the necessity of a multidimensional resilience assessment framework.

3.2.2. Risk propagation under varying numbers of attack nodes

The impact of different shock types and the number of shocked nodes on the efficiency of supply chain networks also varies under different network structures.[73] Figure 5 illustrates changes in supply chain network efficiency under random and targeted attacks across the three network structures, with 10% to 90% of the network impacted.

Figure 5A and 5B illustrate changes in the number of nodes under random and targeted attacks in the random network. A comparative analysis revealed that random networks exhibited extremely low tolerance to risk shocks.[74] Specifically, when the intensity of node shocks increased by 10%, supply chain network efficiency declined sharply. In particular, under targeted attacks, an attack on 10% of nodes propagated eight times within the network. However, when 20% of nodes were targeted, the supply chain network became fully paralyzed after only four propagation steps. Furthermore, when the shock intensity reached 30%, the supply chain network collapsed after merely three steps of risk propagation.[75] Under random attacks, the random network displayed significant vulnerability only when exposed to shocks affecting more than 40% of nodes.

Figure 5C and 5D illustrate changes in the supply chain network efficiency of the small-world network under random and targeted attacks with varying numbers of affected nodes. Unlike random networks, small-world

Table 1. Network resilience under random and targeted attacks on different network structures

Attack type	Network type	T_{50}	AUC	TEV	ADR
Random attack	Random network	Threshold not breached	7.1883	8.1333	0.0122
	Small-world network	5	3.7633	3.3433	0.1111
	Scale-free network	5	2.9833	3.3067	0.1111
Targeted attack	Random network	7	4.9100	5.2633	0.1000
	Small-world network	5	3.3367	3.1400	0.1000
	Scale-free network	3	1.9767	1.9000	0.1000

Abbreviations: ADR: Average decline rate; AUC: Area under the effective node ratio curve; T_{50}: Threshold round of 50% efficiency; TEV: Total effective value.

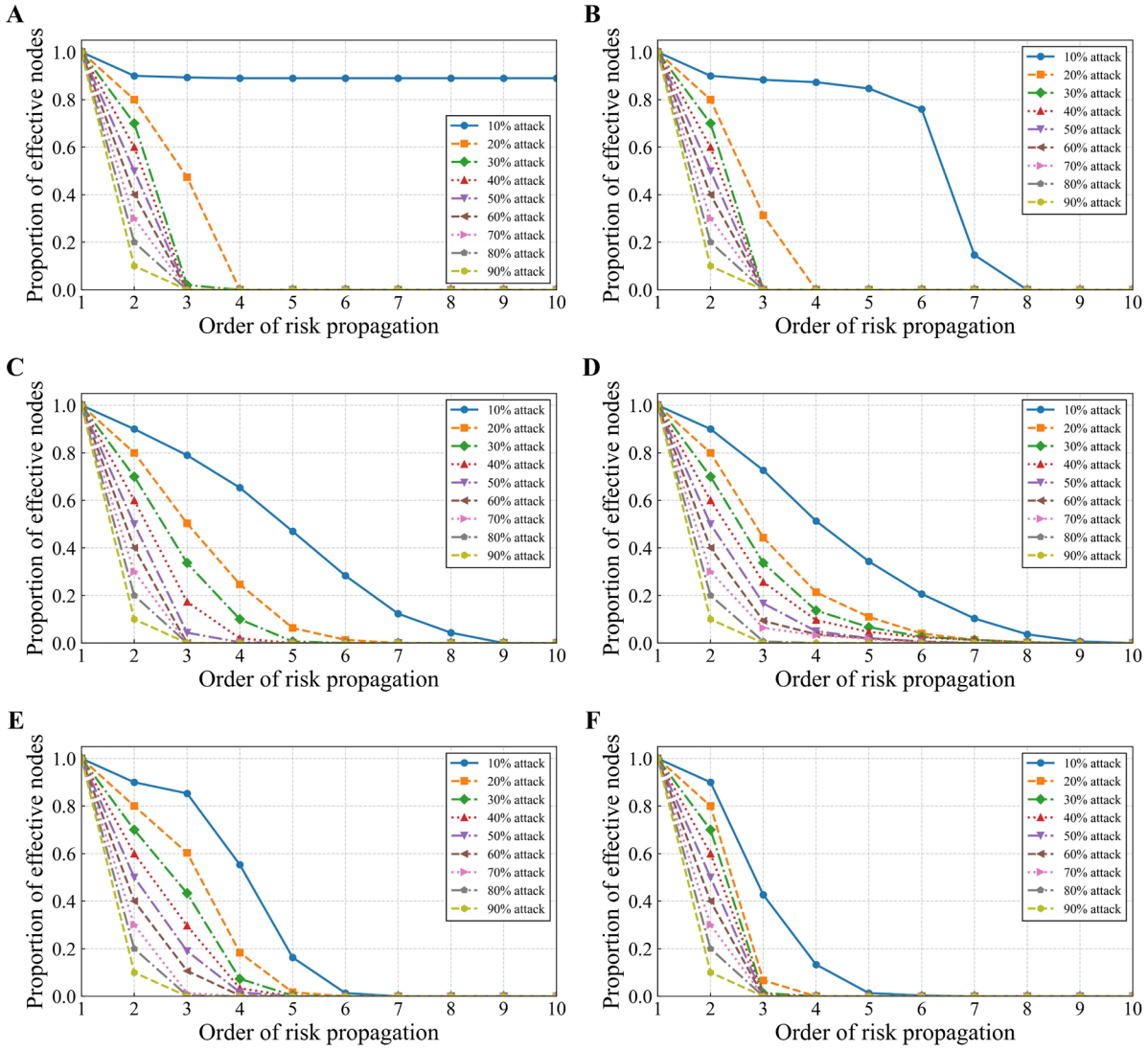

Figure 5. Supply chain network efficiency under varying attack intensities for (A, C, E) random and (B, D, F) targeted attacks. (A & B) Random network. (C & D) Small-world network. (E & F) Scale-free network.

networks exhibited a gradual, stepwise decline in supply chain network efficiency as the number of attacked nodes increased.[76] Under random shocks, an attack targeting 50% of nodes propagated five times within the network. In contrast, under targeted shocks, an attack on 70% of nodes propagated seven times. These results indicate that small-world networks exhibit strong resilience against high-intensity attacks.

By comparing changes in the number of attacked nodes under random and targeted attacks in the scale-free network, as depicted in Figure 5E and 5F, we observed that the scale-free network displayed significant vulnerability under targeted attacks.[77] Specifically, an attack on only 20% of nodes induced a rapid network collapse. Under random shocks, scale-free networks exhibited robustness: increasing the number of attacked nodes did not significantly reduce supply chain network efficiency. Even after 80% of the nodes were attacked, the network could still sustain information propagation for four rounds.

Table 2 presents the resilience profiles of supply chain networks under varying attack intensities, with the 10% node attack scenario serving as the baseline perturbation. The results highlight that both network topology and attack strategy critically shape systemic vulnerability. Under random attacks, all three network types exhibited moderate performance degradation. Notably, the random network did not breach the T_{50} threshold throughout the simulation, underscoring its robustness. In contrast, both small-world and scale-free networks reached T_{50} at round 5, yet maintained moderate levels of AUC and TEV, indicating partial functional retention. Targeted attacks, however, induced substantially more severe disruptions across all structures, with the scale-free network suffering the most pronounced collapse—its T_{50} occurred as early as round 3, accompanied by markedly low AUC (1.9767) and TEV (1.9000)—a direct consequence of its reliance on highly connected hubs. Intriguingly, even under targeted attack, the random network achieved a T_{50} of 7 rounds, outperforming other topologies under random attack, attesting to the resilience advantage conferred by its decentralized architecture. Furthermore, the ADR remained relatively stable across scenarios (ranging from 0.1000 to 0.1429), reinforcing the insight that uniform decay rates can mask significant differences in operational endurance and cumulative functionality. This observation further validates the need for a multidimensional resilience assessment framework that captures not only how fast a system degrades but also how long and how well it sustains effective operations before failure.

3.2.3. Risk propagation under different load capacities

The strategic resilience parameter β and the external dependence parameter γ jointly affect the load capacity of nodes.[78] Assuming the initial number of impacted and failed nodes remained fixed at 20, we simulated changes in supply chain network efficiency under the three network structures and the two attack modes across various parameter settings. This study aims to investigate the propagation of carbon reduction risks within manufacturing supply chain networks.

Figure 6 illustrates the impact of load-capacity variations under random and targeted attacks on supply chain network efficiency in a random network: random attack with $\gamma = 0.7$ and β varies (Figure 6A), random attack with $\beta = 0.3$ and γ varies (Figure 6B), targeted attack with $\gamma = 0.7$ and β varies (Figure 6C), and targeted attack with $\beta = 0.3$ and γ varies (Figure 6D). As shown in Figure 6, when the external dependency parameter γ was held constant, supply chain network resilience increased with increasing strategic resilience parameter β. Conversely, when the strategic resilience parameter β was fixed, a smaller value of the external dependence parameter γ led to a milder decline in network efficiency and a lower probability of network failure and paralysis.[79] The results demonstrate that targeted attacks generate substantially greater vulnerability relative to random attacks.[80] These findings are consistent with conclusions from prior studies using distinct analytical methods: one[81] focusing on network structural configurations and the other on target node characteristics.[82]

Table 3 presents the resilience metrics of random supply chain networks under four distinct attack regimes—β-random, γ-random, β-targeted, and γ-targeted—as the strategic resilience parameter β and the external dependence parameter γ are systematically varied. The results demonstrate that network performance is highly sensitive to both internal adaptive capacity and external interdependence. Under β-random attacks, increasing β consistently improved resilience: T50 rose from round 3 ($\beta = 0.1$) to round 5 ($\beta = 0.2$), and for $\beta \geq 0.3$, T50 was never breached, with AUC and TEV stabilizing at 3.65 and 4.60, respectively. These findings indicate that a higher strategic resilience parameter enhances the ability to withstand random disruptions and substantially postpones the onset of functional degradation. In contrast, under γ-random attacks, increasing γ led to earlier collapse—T50 shifted from "not breached" at $\gamma = 0.1$ to round 3 at $\gamma = 0.3$—with corresponding declines in AUC and

Table 2. Network resilience under 10% attack intensity

Network type	Attack type	Percentage of nodes attacked	T_{50}	AUC	TEV	ADR
Random network	Random attack	10% attack	Threshold not breached	2.7383	3.6833	0.0275
	Targeted attack	10% attack	7	4.9100	5.2633	0.1250
Scale-free network	Random attack	10% attack	5	2.9833	3.3067	0.1429
	Targeted attack	10% attack	3	1.9767	1.9000	0.1429
Small-world network	Random attack	10% attack	5	3.7633	3.3433	0.1111
	Targeted attack	10% attack	5	3.3367	3.1400	0.1000

Note: The full simulation covers attack scenarios ranging from 10% to 90% of nodes compromised, yielding 54 experimental configurations (6 network–attack combinations × 9 attack levels). To conserve space, only the results for the 10% attack scenario—the mildest perturbation—are presented here, as it provides a baseline for comparing intrinsic network resilience under minimal disruption. Under random attacks, the random network does not breach the failure threshold (i.e., T_{50} is never reached), and risk propagation ceases as early as round 4. Consequently, although its AUC and TEV values are lower in absolute terms compared to other scenarios, this reflects early stabilization and the absence of prolonged functional degradation.
Abbreviations: ADR: Average decline rate; AUC: Area under the effective node ratio curve; T_{50}: Threshold round of 50% efficiency; TEV: Total effective value.

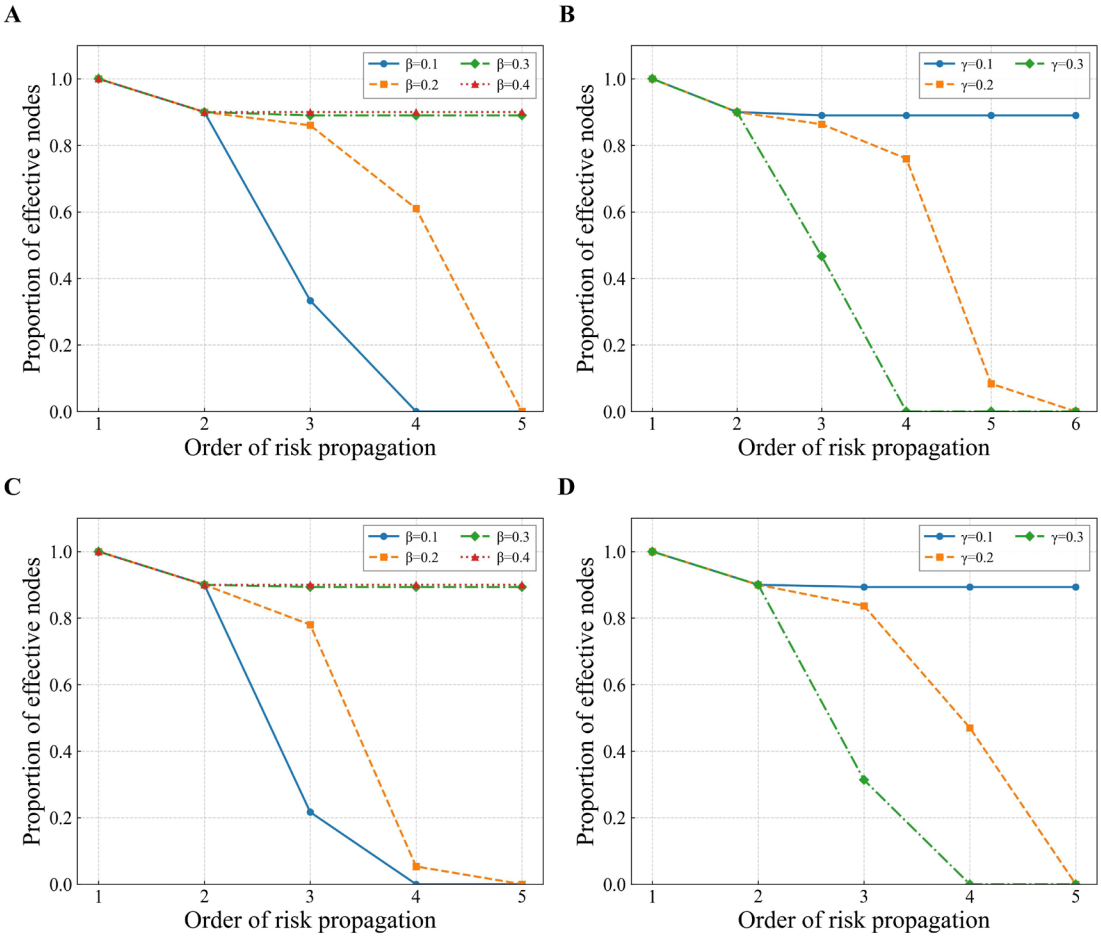

Figure 6. Supply chain network efficiency under different load capacities in random networks. (A) β-random attack. (B) γ-random attack. (C) β-targeted attack. (D) γ-targeted attack.

TEV, suggesting that stronger individual firm resilience cannot offset systemic fragility when partner failures propagate through dense interdependencies. Similar patterns emerged under targeted attacks: in β-targeted and γ-targeted scenarios, moderate strategic resilience parameter values yielded optimal resilience, while higher values often accelerated failure, particularly when attacks exploited relational vulnerabilities. Notably, the ADR remained largely invariant across configurations (0.1667 or 0.2000), underscoring its limited discriminative power compared to trajectory-based indicators such as T50, AUC, and TEV. These results highlight that while enhancing strategic resilience can bolster robustness against random shocks, the effectiveness of such strategies depends on the attack type and the underlying structure of inter-firm dependencies.

Figure 7 illustrates the impact of load-capacity variations under random and targeted attacks on network efficiency in small-world networks. Figure 7A and 7C illustrate the network efficiency in small-world networks for varying values of β when γ = 0.7. When γ was constant, the number of risk shocks the supply chain network could withstand gradually increased as the strategic resilience parameter β rose.[83] Moreover, targeted attacks amplified the influence of parameter changes on supply chain network efficiency.[84] When the strategic resilience parameter β increased to 0.5 with γ fixed, the resilience of supply chain nodes against targeted attacks improved by approximately 20%.

Figure 7B and 7D illustrate the impact of changes in γ on supply chain network efficiency when β = 0.3. When β was held constant, the network became more prone to rapid collapse under external risk shocks as the external dependence parameter γ increased. When firms maintained γ at or below 0.5, this exerted a significantly positive effect on the risk resilience of the supply chain network.[85] In addition, small-world networks failed sooner and more rapidly under targeted attacks than under random attacks, highlighting the greater vulnerability of supply chain networks to targeted disruptions.

Table 4 reports the resilience metrics of small-world supply chain networks under four attack regimes—β-random, γ-random, β-targeted, and γ-targeted attacks—as the strategic resilience parameter β and external dependency parameter γ were systematically varied. The results demonstrate that small-world networks exhibit strong baseline robustness: under β-random attacks, increasing β from 0.1 to 0.8 consistently delayed or stabilized functional collapse, with T_{50} plateauing at 6 rounds for β ≥ 0.3 and AUC/TEV values steadily rising before saturating near 5.05 and 4.06, respectively. This confirms that enhancing firms' strategic resilience capacity (higher β) effectively mitigates random disruptions. In contrast, under γ-random attacks, a higher γ paradoxically correlated with earlier failure when β was fixed—T50 dropped from 6 (at γ = 0.1) to 4 (at γ = 0.7)—suggesting that in highly interdependent settings, even resilient firms

Table 3. Network resilience under different load capacities in random networks

Group	Parameter	T_{50}	AUC	TEV	ADR
β-random attack	β = 0.1	3	1.7333	1.9000	0.2000
	β = 0.2	5	2.8700	3.3700	0.2000
	β = 0.3	Threshold not breached	3.6250	4.5700	0.0220
	β = 0.4	Threshold not breached	3.6500	4.6000	0.0200
γ-random attack	γ = 0.1	Threshold not breached	4.5150	5.4600	0.0183
	γ = 0.2	5	3.1067	3.5233	0.1667
	γ = 0.3	3	1.8667	1.9000	0.1667
β-targeted attack	β = 0.1	3	1.6167	1.9000	0.2000
	β = 0.2	4	2.2333	2.6800	0.2000
	β = 0.3	Threshold not breached	3.6333	4.5800	0.0213
	β = 0.4	Threshold not breached	3.6500	4.6000	0.0200
γ-targeted attack	γ = 0.1	Threshold not breached	3.6333	4.5800	0.0213
	γ = 0.2	4	2.7067	2.7367	0.2000
	γ = 0.3	3	1.7133	1.9000	0.2000

Abbreviations: ADR: Average decline rate; AUC: Area under the effective node ratio curve; T_{50}: Threshold round of 50% efficiency; TEV: Total effective value.

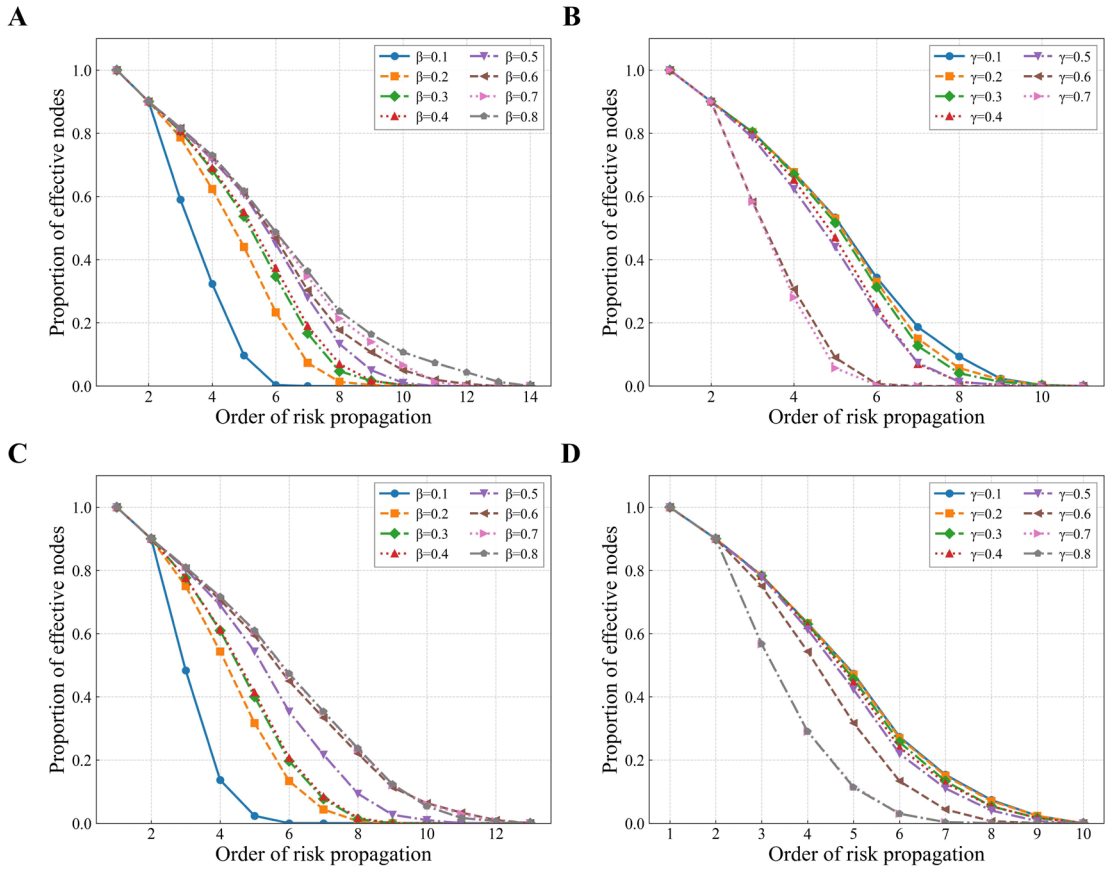

Figure 7. Supply chain network efficiency under different load capacities in small-world networks. (A) β-random attack. (B) γ-random attack. (C) β-targeted attack. (D) γ-targeted attack. Note: To examine the impact of key parameter variations in supply chain networks, we systematically varied the strategic resilience parameter β and external dependency parameter γ over the range [0.1, 0.9]. However, during simulations, we observed that for certain (β, γ) combinations, the system either reached an absorbing state—where risk propagation ceased due to exhaustion of susceptible nodes—or underwent complete collapse via cascading failure. In both cases, further simulation rounds yielded no new dynamics, as the supply chain network state remained unchanged. To improve computational efficiency and avoid redundant iterations, the simulation was terminated once convergence or total failure was confirmed.

cannot fully offset systemic fragility triggered by partner failures. Under targeted attacks, the supply chain network showed greater sensitivity to γ than to β: under β-targeted attacks, increasing β improved resilience (T50 remained at 6 for $\beta \geq 0.5$), whereas under γ-targeted attacks, increasing γ beyond 0.5 led to a sharp decline in performance (T50 fell from 5 to 4, and AUC dropped from 3.59 to 2.40), indicating that targeting highly dependent nodes severely undermines supply chain network stability regardless of individual firm resilience. Notably, ADR remained remarkably stable across all configurations (ranging from 0.0714 to 0.1000), reinforcing the idea that the average decay rate alone fails to capture critical differences in operational endurance. These findings highlight that while small-world topology confers inherent robustness against random shocks, its vulnerability under targeted attacks—especially those exploiting relational dependencies—necessitates careful balancing of strategic resilience investment and external dependence risk management.

Figure 8 illustrates the impact of load-capacity variations under random and targeted attacks on supply chain network efficiency in scale-free networks. By comparing Figure 8A and 8C, under random attacks with γ held constant, the supply chain network exhibited greater resilience as the strategic resilience parameter β increased. Compared with random attacks, targeted attacks exerted a particularly strong impact on supply chains in scale-free networks. When firms' external dependence remained constant, a rise in the strategic resilience parameter β did not improve supply chain risk resilience.

As shown in Figure 8B and 8D, a decrease in firms' external dependence parameter γ enhanced resilience to a certain extent, thereby improving the risk-resistance capacity of the supply chain network.[86] In contrast, targeted attacks exposed the vulnerability of the supply chain

Table 4. Network resilience under different load capacities in small-world networks

Group	Parameter	T_{50}	AUC	TEV	ADR
β-random attack	β = 0.1	4	2.4133	2.4900	0.0714
	β = 0.2	5	3.5733	3.3100	0.0714
	β = 0.3	6	4.0067	3.9267	0.0714
	β = 0.4	6	4.1000	3.9467	0.0714
	β = 0.5	6	4.4600	4.0367	0.0714
	β = 0.6	6	4.6833	4.0533	0.0714
	β = 0.7	6	4.8200	4.0567	0.0714
	β = 0.8	6	5.0500	4.0633	0.0714
γ-random attack	γ = 0.1	6	4.0633	3.9133	0.0909
	γ = 0.2	6	3.9700	3.9100	0.0909
	γ = 0.3	6	3.8867	3.8900	0.0909
	γ = 0.4	5	3.6567	3.3500	0.0909
	γ = 0.5	5	3.5733	3.3100	0.0909
	γ = 0.6	4	2.3867	2.4833	0.0909
	γ = 0.7	4	2.3233	2.4833	0.0909
β-targeted attack	β = 0.1	3	2.0433	1.9000	0.0769
	β = 0.2	5	3.1933	3.1933	0.0769
	β = 0.3	5	3.4733	3.2867	0.0769
	β = 0.4	5	3.5100	3.2900	0.0769
	β = 0.5	6	4.1367	3.9367	0.0769
	β = 0.6	6	4.7300	4.0067	0.0769
	β = 0.7	6	4.8067	4.0333	0.0769
	β = 0.8	6	4.8000	4.0367	0.0769
γ-targeted attack	γ = 0.1	5	3.8133	3.3167	0.1000
	γ = 0.2	5	3.8000	3.3167	0.1000
	γ = 0.3	5	3.7300	3.3133	0.1000
	γ = 0.4	5	3.6933	3.3100	0.1000
	γ = 0.5	5	3.5933	3.2933	0.1000
	γ = 0.6	5	3.1933	3.1933	0.1000
	γ = 0.7	4	2.4067	2.4667	0.1000
	γ = 0.8	4	2.4033	2.4667	0.1000

Abbreviations: ADR: Average decline rate; AUC: Area under the effective node ratio curve; T_{50}: Threshold round of 50% efficiency; TEV: Total effective value.

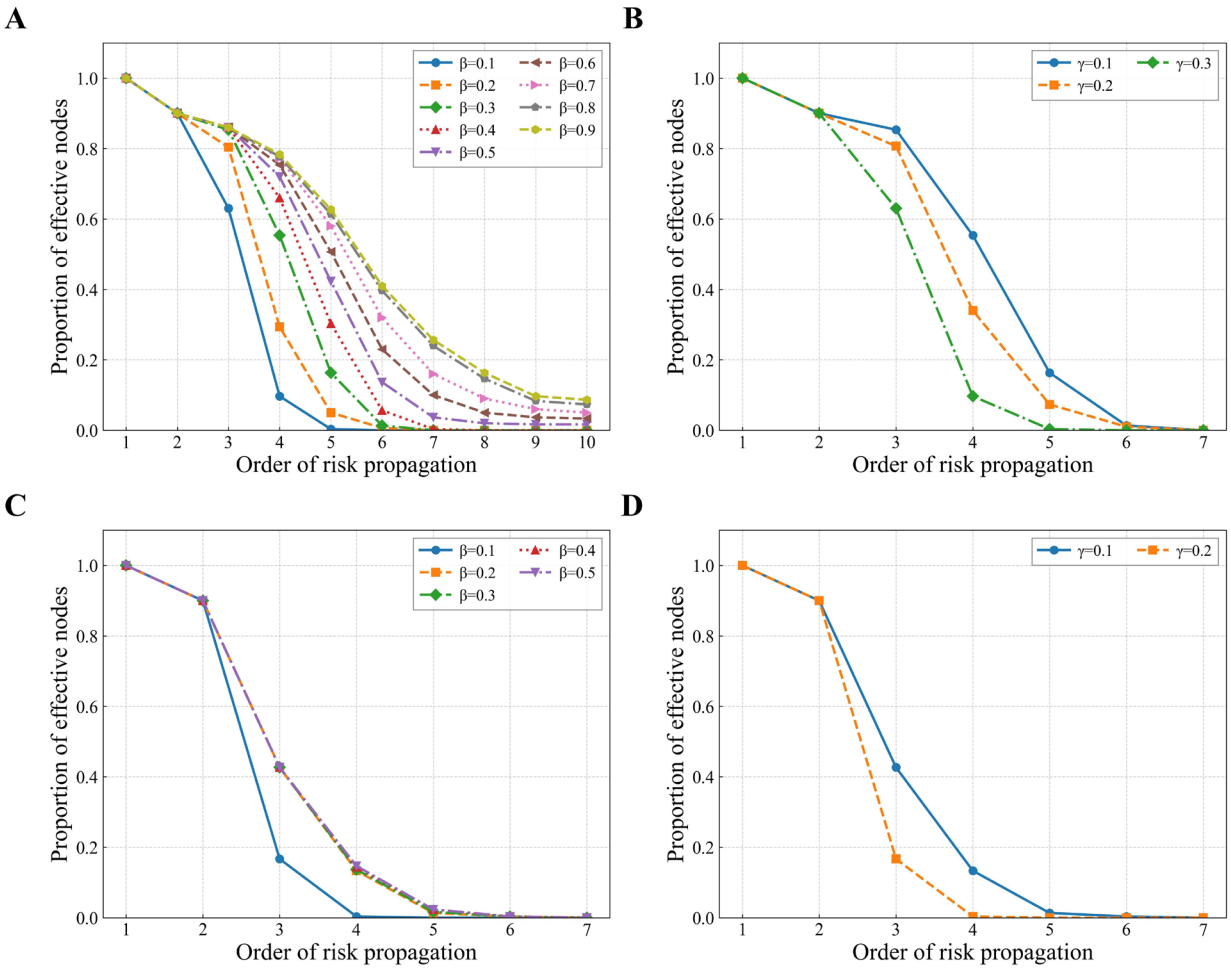

Figure 8. Supply chain network efficiency under different load capacities in scale-free networks. (A) β-random attack. (B) γ-random attack. (C) β-targeted attack. (D) γ-targeted attack.

network, making the effect of changes in parameter γ on network efficiency less significant. Through a comparative analysis of load-bearing capacity dynamics across three distinct network structures, this study reveals that the failure probability of supply chain networks exhibits an inverse relationship with firms' strategic resilience parameter β. Furthermore, the analysis showed that this failure probability is directly proportional to the external dependency parameter γ.

Table 5 presents the resilience performance of scale-free supply chain networks under four attack scenarios—β-random, γ-random, β-targeted, and γ-targeted—with the non-attack parameter systematically varied in each case. Under β-random attacks, higher values of β substantially enhanced network resilience: T50 improved from round 4 to round 6, with AUC and TEV stabilizing around 4.64 and 4.17, respectively. This reflects the protective effect of greater tolerance or operational buffers against random failures governed by strategic resilience rules. In contrast, under γ-random attacks, increasing γ led to earlier functional collapse, indicating that stronger individual crisis response capacity cannot offset systemic risk when failures propagate through relational dependencies. Under both targeted attack regimes, the network exhibited substantially weaker performance: T_{50} collapsed to round 3 across all parameter settings, while AUC and TEV fell to markedly low levels, indicating minimal sustained operational capacity. Moreover, the ADR increased relative to random attack scenarios reflecting a faster and more severe attenuation of effective functionality. These results confirm that scale-free networks are especially vulnerable to targeted disruptions, in which the removal of central or highly dependent nodes triggers rapid and extensive cascading failures that cannot be mitigated by adjusting β or γ alone.

Table 5. Network resilience under different load capacities in scale-free networks

Group	Parameter	T_{50}	AUC	TEV	ADR
β-random attack	β = 0.1	4	2.1300	2.5300	0.1000
	β = 0.2	4	2.5533	2.7033	0.1000
	β = 0.3	5	2.9833	3.3067	0.1000
	β = 0.4	5	3.2833	3.4200	0.1000
	β = 0.5	5	3.6217	3.4800	0.0983
	β = 0.6	6	3.9533	4.0200	0.0967
	β = 0.7	6	4.2683	4.1133	0.0950
	β = 0.8	6	4.5533	4.1500	0.0927
	β = 0.9	6	4.6400	4.1700	0.0913
γ-random attack	γ = 0.1	5	2.9833	3.3067	0.1429
	γ = 0.2	4	2.6300	2.7067	0.1429
	γ = 0.3	4	2.1300	2.5300	0.1429
β-targeted attack	β = 0.1	3	1.5700	1.9000	0.1429
	β = 0.2	3	1.9767	1.9000	0.1429
	β = 0.3	3	1.9833	1.9000	0.1429
	β = 0.4	3	1.9967	1.9000	0.1429
	β = 0.5	3	2.0000	1.9000	0.1429
γ-targeted attack	γ = 0.1	3	1.9767	1.9000	0.1429
	γ = 0.2	3	1.5700	1.9000	0.1429

Abbreviations: ADR: Average decline rate; AUC: Area under the effective node ratio curve; T_{50}: Threshold round of 50% efficiency; TEV: Total effective value.

4. Conclusion

Drawing on complex network theory, this study develops a benchmark model for multi-stage industrial chain segmentation to investigate the determinants of firm positioning in supply chain networks. The analysis identified four key drivers: pricing strategy, production costs, transportation costs, and investment in carbon reduction.

The study first establishes the theoretical mechanism of risk propagation. Carbon reduction risks propagate through the supply chain by increasing unit production costs, leading to higher product prices and reduced supply to downstream firms. This, in turn, depresses procurement demand. Due to the clustered and complex structure of supply chain networks, such effects generate bidirectional risk transmission along both upstream and downstream directions. Building on this theoretical foundation, numerical simulations were conducted to examine the dynamic propagation of carbon reduction risks, yielding three principal findings regarding network resilience, efficiency, and adaptive capacity:

(i) Network resilience varies by structure and shock type. Under random attacks, random networks are most robust, followed by scale-free networks, while small-world networks are the least resilient. Under targeted attacks, however, small-world networks perform best, followed by random networks, with scale-free networks being the most vulnerable. Across all types, random attacks are less damaging than targeted ones. Targeted attacks cause earlier and faster degradation, with scale-free networks collapsing most severely due to their reliance on hub nodes.

(ii) Supply chain efficiency declines sharply in random networks even with a few shocked nodes, while in small-world networks the decline is more gradual. Scale-free networks are highly susceptible to

targeted attacks but resilient to random disruptions, with minimal efficiency loss as the scale of attacks increases. Across all networks, a 10% random attack yields moderate performance decline, whereas the same level of targeted attack—especially in scale-free networks—triggers severe efficiency loss, with the 50% threshold reached early.

(iii) Supply chain resilience is influenced by firms' strategic resilience and their external dependence. Higher strategic resilience enhances network resilience under random attacks, whereas greater external dependence leads to earlier systemic collapse. In random networks, moderate parameter values generate optimal resilience under targeted attacks, while excessive values amplify relational vulnerabilities. In smallworld networks, the structure is more sensitive to external dependence than to strategic resilience, and targeting highly dependent nodes severely undermines stability. In scalefree networks, the structure is highly vulnerable to targeted attacks, triggering rapid cascading failures across all parameter settings. Adjustments in either strategic resilience or external dependence alone cannot prevent systemic collapse caused by disruptions to central nodes.

Acknowledgments

None.

Funding

The study was financially supported by the General Project of Hubei Provincial Social Science Fund (HBSKJJ20253229), the Project of Hubei Provincial Department of Education (24Q072, 24Y046), and the Young Scientists Fund of National Natural Science Foundation of China (72303127).

Conflict of interest

The authors reported no conflict of interest.

Author contributions

Conceptualization: He Yu, Chen Zhenzhen
Methodology: He Yu, Tian Jiexin
Writing–original draft: Shu Siqin, Chen Zhenzhen
Writing–review & editing: He Yu, Chen Zhenzhen, Shu Siqin

Availability of data

The data can be obtained from the corresponding author upon request.

References

1. Sgaravatti G, Tagliapietra S, Trasi C. Europe's fiscal policy response to the energy crisis: lessons learned for a greener way out. *Energy Efficiency*. 2024;17(8):90.

doi: 10.1007/s12053-024-10275-0

2. Wu X, Li Z, Tang F. The effect of carbon price volatility on firm green transitions: Evidence from Chinese manufacturing listed firms. *Energies*. 2022;15(20):7456.

doi: 10.3390/en15207456

3. Liu C, Yang Y, Chen S. How does transition finance influence green innovation of high-polluting and high-energy-consuming firms? Evidence from China. *Environ Sci Pollut Res*. 2024;31(6):8026-8045.

doi: 10.1007/s11356-023-31360-4

4. Ge K, Xu H, Liu X. Green transition of urban land use: Spatial spillover effects and boundaries on urban land use efficiency. *Environ Dev Sustain*. 2025;27(2):4037-4054.

doi: 10.1007/s10668-025-07022-5

5. Shayegh S, Reissl S, Roshan E, Calcaterra M. An assessment of different transition pathways to a green global economy. *Commun Earth Environ*. 2023;4(1):448.

doi: 10.1038/s43247-023-01109-5

6. Basilico S, Grashof N. Accelerating the sustainability transition of brown regions: Unlocking the speed factor. *Environ Innov Soc Transitions*. 2024;51:100840.

doi: 10.1016/j.eist.2024.100840

7. Aydin M, Degirmenci T, Ahmed Z, Apergis N. Do the energy taxes, green technological innovation, and energy productivity enable the green energy transition in EU countries? Evidence from novel panel data estimators. *Renew Energy*. 2025;249:123236.

doi: 10.1016/j.renene.2025.123236

8. Aziz G, Sarwar S. Revisit the role of governance indicators to achieve sustainable economic growth of Saudi Arabia - pre and post implementation of 2030 Vision. *Struct Change Econ Dyn*. 2023;66:213-227.

doi: 10.1016/j.strueco.2023.04.008

9. Aziz G, Waheed R, Sarwar S, Khan MS. The Significance of Governance Indicators to Achieve Carbon Neutrality: A New Insight of Life Expectancy. *Sustainability*. 2022;15(1):766.

doi: 10.3390/su15010766

10. Meng X, Wu C. Empirical evidence on digitization enabling the transition to a green economy in China. *Environ Sci Pollut Res*. 2024;31(37):51790-51805.

doi: 10.1007/s11356-024-34613-y

11. Li Y, Yang X, Du E, *et al.* A review on carbon emission accounting approaches for the electricity power industry. *Appl Energy*. 2024;359:122681.

doi: 10.1016/j.apenergy.2024.122681

12. McDowall W, Geng Y, Huang B, *et al*. Circular economy policies in China and Europe. *J Ind Ecol*. 2017;21(3):651-661.

doi: 10.1111/jiec.12597

13. Zhai X, An Y, Shi X, Liu X. Measurement of green transition and its driving factors: Evidence from China. *J Clean Prod*. 2022;335:130292.

doi: 10.1016/j.jclepro.2021.130292

14. Chen W, Zou W, Zhong K, Aliyeva A. Machine learning assessment under the development of green technology innovation: A perspective of energy transition. *Renew Energy*. 2023;214:65-73.

doi: 10.1016/j.renene.2023.05.108

15. Lüdeke-Freund F, Gold S, Bocken NMP. A review and typology of circular economy business model patterns. *J Ind Ecol*. 2019;23(1):36-61.

doi: 10.1111/jiec.12763

16. Tong X. The spatiotemporal evolution pattern and influential factor of regional carbon emission convergence in China. *Adv Meteorol*. 2020;2020:4361570.

doi: 10.1155/2020/4361570

17. Köveker T, Chiappinelli O, Kröger M, *et al*. Green premiums are a challenge and an opportunity for climate policy design. *Nat Clim Chang*. 2023;13(7):592-595.

doi: 10.1038/s41558-023-01689-2

18. Huang W, Wang Q, Li H, Fan H, Qian Y, Klemeš JJ. Review of recent progress of emission trading policy in China. *J Clean Prod*. 2022;349:131480.

doi: 10.1016/j.jclepro.2022.131480

19. Yang Y, Chi Y. Path selection for enterprises' green transition: Green innovation and green mergers and acquisitions. *J Clean Prod*. 2023;412:137397.

doi: 10.1016/j.jclepro.2023.137397

20. Sun C, Li Z, Ma T, He R. Carbon efficiency and international specialization position: Evidence from global value chain position index of manufacture. *Energy Policy*. 2019;128:235-242.

doi: 10.1016/j.enpol.2018.12.058

21. Quader MA, Ahmed S, Ghazilla RAR, Ahmed S, Dahari M. A comprehensive review on energy efficient CO2 breakthrough technologies for sustainable green iron and steel manufacturing. *Renew Sustain Energy Rev*. 2015;50:594-614.

doi: 10.1016/j.rser.2015.05.026

22. Osório A. Not everything is green in the green transition: Theoretical considerations on market structure, prices and competition. *J Clean Prod*. 2023;427:139300.

doi: 10.1016/j.jclepro.2023.139300

23. Ma R, Lin Y, Lin B. Does digitalization support green transition in Chinese cities? Perspective from Metcalfe's Law. *J Clean Prod*. 2023;425:138769.

doi: 10.1016/j.jclepro.2023.138769

24. Kjaer LL, Pigosso DCA, Niero M, Bech NM, McAloone TC. Product/Service-Systems for a circular economy: The route to decoupling economic growth from resource consumption? *J Ind Ecol*. 2019;23(1):22-35.

doi: 10.1111/jiec.12747

25. Wang K. The effect of transition finance on ESG performance: Empirical evidence from China's high-carbon industries. *Int J Low-Carbon Technol*. 2025;20:1809-1817.

doi: 10.1093/ijlct/ctaf113

26. Wang Y, Liu J, Zhao Z, Ren J, Chen X. Research on carbon emission reduction effect of China's regional digital trade under the "double carbon" target combination of the regulatory role of industrial agglomeration and carbon emissions trading mechanism. *J Clean Prod*. 2023;405:137049.

doi: 10.1016/j.jclepro.2023.137049

27. Shobande OA, Tiwari AK, Ogbeifun L. Quantifying the role of the energy transition in alleviating marginalisation and advancing inclusive green growth. *J Environ Manage*. 2025;390:126241.

doi: 10.1016/j.jenvman.2025.126241

28. Hielscher S, Sovacool BK. Contested smart and low-carbon energy futures: Media discourses of smart meters in the United Kingdom. *J Clean Prod*. 2018;195:978-990.

doi: 10.1016/j.jclepro.2018.05.227

29. Unruh GC. The real stranded assets of carbon lock-in. *One Earth*. 2019;1(4):399-401.

doi: 10.1016/j.oneear.2019.11.012

30. Unruh GC, Carrillo-Hermosilla J. Globalizing carbon lock-in. *Energy Policy*. 2006;34(10):1185-1197.

doi: 10.1016/j.enpol.2004.10.013

31. Li J, Li S. Energy investment, economic growth and carbon emissions in China-Empirical analysis based on spatial Durbin model. *Energy Policy*. 2020;140:111425.

doi: 10.1016/j.enpol.2020.111425

32. Tvinnereim E, Mehling M. Carbon pricing and deep decarbonisation. *Energy Policy*. 2018;121:185-189.

doi: 10.1016/j.enpol.2018.06.020

33. Zhao R, Gao J, Lyu X, *et al*. How does green transition of farmland use affect grain production capacity? Evidence from China. *Reg Environ Change*. 2025;25(4):153.

doi: 10.1007/s10113-025-02483-w

34. Watson M, Machado P, Da Silva A, *et al*. Sustainable aviation

fuel technologies, costs, emissions, policies, and markets: A critical review. *J Clean Prod*. 2024;449:141472.

doi: 10.1016/j.jclepro.2024.141472

35. Galan M, Lindner R. To get the European transition to green hydrogen right, equitable partnerships with the Global South matter. *Environ Sci Policy*. 2025;168:104066.

doi: 10.1016/j.envsci.2025.104066

36. Sun W, Huang C. Predictions of carbon emission intensity based on factor analysis and an improved extreme learning machine from the perspective of carbon emission efficiency. *J Clean Prod*. 2022;338:130414.

doi: 10.1016/j.jclepro.2022.130414

37. McGill E, Er V, Penney T, *et al*. Evaluation of public health interventions from a complex systems perspective: A research methods review. *Soc Sci Med*. 2021;272:113697.

doi: 10.1016/j.socscimed.2021.113697

38. Abrol A, Fu Z, Salman M, *et al*. Deep learning encodes robust discriminative neuroimaging representations to outperform standard machine learning. *Nat Commun*. 2021;12(1):353.

doi: 10.1038/s41467-020-20655-6

39. Song X, Jia X, Dong Q, Xu D. System reliability under cascading failure models with different load effect modes. *Qual Reliab Eng Int*. 2023;39(6):2094-2112.

doi: 10.1002/qre.3304

40. Swift AW. Stochastic models of cascading failures. *J Appl Probab*. 2008;45(4):907-921.

doi: 10.1239/jap/1231340223

41. Wang Y, Zhang F. Modeling and analysis of under-load-based cascading failures in supply chain networks. *Nonlinear Dyn*. 2018;92(3):1403-1417.

doi: 10.1007/s11071-018-4135-z

42. Zhao K, Zuo Z, Blackhurst JV. Modelling supply chain adaptation for disruptions: An empirically grounded complex adaptive systems approach. *J Oper Manag*. 2019;65(2):190-212.

doi: 10.1002/joom.1009

43. Bode C, Wagner SM. Structural drivers of upstream supply chain complexity and the frequency of supply chain disruptions. *J Oper Manag*. 2015;36(1):215-228.

doi: 10.1016/j.jom.2014.12.004

44. Alkahtani H, Aldhyani TH. Intrusion detection system to advance internet of things infrastructure-based deep learning algorithms. *Complexity*. 2021;2021:5579851.

doi: 10.1155/2021/5579851

45. Zhang Z, Zhu Y, Yang T, Li L, Zhu H, Wang H. Conversion of local industrial wastes into greener cement through geopolymer technology: A case study of high-magnesium nickel slag. *J Clean Prod*. 2017;141:463-471.

doi: 10.1016/j.jclepro.2016.09.147

46. Zhang T, Uratani J, Huang Y, Xu L, Griffiths S, Ding Y. Hydrogen liquefaction and storage: Recent progress and perspectives. *Renew Sustain Energy Rev*. 2023;176:113204.

doi: 10.1016/j.rser.2023.113204

47. Moosavi J, Fathollahi-Fard AM, Dulebenets MA. Supply chain disruption during the COVID-19 pandemic: Recognizing potential disruption management strategies. *Int J Disaster Risk Reduct*. 2022;75:102983.

doi: 10.1016/j.ijdrr.2022.102983

48. Pérez-Fortes M, Schöneberger JC, Boulamanti A, Tzimas E. Methanol synthesis using captured CO2 as raw material: Techno-economic and environmental assessment. *Appl Energy*. 2015;161:718-732.

doi: 10.1016/j.apenergy.2015.07.067

49. Ma X, Khan MN, Awosusi AA, Uzun B, Shamansurova Z. Heterogeneous impact of green energy innovation on energy transition in the G7 nations: an aggregated and disintegrated analysis through advanced quantile approach. *Int J Sustain Dev World Ecol*. 2024;31(3):264-278.

doi: 10.1080/13504509.2023.2277422

50. Ivanov D, Dolgui A, Sokolov B, Ivanova M. Literature review on disruption recovery in the supply chain. *Int J Prod Res*. 2017;55(20):6158-6174.

doi: 10.1080/00207543.2017.1330572

51. Liao S, Hu D, Ding L. Assessing the influence of supply chain collaboration value innovation, supply chain capability and competitive advantage in Taiwan's networking communication industry. *Int J Prod Econ*. 2017;191:143-153.

doi: 10.1016/j.ijpe.2017.06.001

52. Tsolakis N, Goldsmith AT, Aivazidou E, Kumar M. Microalgae-based circular supply chain configurations using Industry 4.0 technologies for pharmaceuticals. *J Clean Prod*. 2023;395:136397.

doi: 10.1016/j.jclepro.2023.136397

53. Dolgui A, Gusikhin O, Ivanov D, Li X, Stecke K. A network-of-networks adaptation for cross-industry manufacturing repurposing. *IISE Trans*. 2024;56(6):666-682.

doi: 10.1080/24725854.2023.2253881

54. Pham T, Yenradee P. Optimal supply chain network design with process network and BOM under uncertainties: A case study in toothbrush industry. *Comput Ind Eng*. 2017;108:177-191.

doi: 10.1016/j.cie.2017.04.012

55. Antràs P, Gortari A. On the geography of global value chains. *Econometrica*. 2020;88(4):1553-1598.

doi: 10.3982/ecta15362

56. Makris S, Zoupas P, Chryssolouris G. Supply chain control logic for enabling adaptability under uncertainty. *Int J Prod Res*. 2011;49(1):121-137.

doi: 10.1080/00207543.2010.508940

57. Shapiro JF. Challenges of strategic supply chain planning and modeling. *Comput Chem Eng*. 2004;28(6-7):855-861.

doi: 10.1016/j.compchemeng.2003.09.013

58. Saha S, Nielsen IE, Moon I. Strategic inventory and pricing decision for substitutable products. *Comput Ind Eng*. 2021;160:107570.

doi: 10.1016/j.cie.2021.107570

59. Huang D. An algorithm to generate all d-lower boundary points for a stochastic flow network using dynamic flow constraints. *Reliab Eng Syst Saf*. 2024;249:110217.

doi: 10.1016/j.ress.2024.110217

60. Liang X, Bao D, Yang Z. State evaluation method for complex task network models. *Inf Sci*. 2023;653:119796.

doi: 10.1016/j.ins.2023.119796

61. Yang Y, Chen J. Comprehensive analysis of water carrying capacity based on wireless sensor network and image texture of feature extraction. *Alex Eng J*. 2022;61(4):2877-2886.

doi: 10.1016/j.aej.2021.08.018

62. Huang S, Hua Z, Wang P, Shi J. A novel longitudinal connectivity index to evaluate reticular river networks based on the combination of network maximum flow and resistance distance. *J Environ Manage*. 2024;367:122062.

doi: 10.1016/j.jenvman.2024.122062

63. Wang L, Cheng L, Liu Y. Uncertainty-oriented physics-informed long short-term memory (UOPI-LSTM) network framework for dynamic force identification with interval uncertainties. *Expert Syst Appl*. 2025;274:127067.

doi: 10.1016/j.eswa.2025.127067

64. Gao T, Yang J, Tang Q. A multi-source domain information fusion network for rotating machinery fault diagnosis under variable operating conditions. *Inf Fusion*. 2024;106:102278.

doi: 10.1016/j.inffus.2024.102278

65. Wang L, Yang Y, Xu L, Ren Z, Fan S, Zhang Y. A particle swarm optimization-based deep clustering algorithm for power load curve analysis. *Swarm Evol Comput*. 2024;89:101650.

doi: 10.1016/j.swevo.2024.101650

66. Cats O, Koppenol G, Warnier M. Robustness assessment of link capacity reduction for complex networks: Application for public transport systems. *Reliab Eng Syst Saf*. 2017;167:544-553.

doi: 10.1016/j.ress.2017.07.009

67. Salama M, El-Dakhakhni W, Tait M. Systemic risk mitigation strategy for power grid cascade failures using constrained spectral clustering. *Int J Crit Infrastruct Prot*. 2023;42:100622.

doi: 10.1016/j.ijcip.2023.100622

68. Zhang W, Luo Z. Research on intercity travel mode recognition and network structure characteristics based on complex network and random forest classification. *Sci Rep*. 2025;15(1):35339.

doi: 10.1038/s41598-025-19392-x

69. Liu Q, Adriaens P. Unraveling risk propagation in the copper value chain: A firm-level network analysis. *Resour Conserv Recycl*. 2025;222:108435.

doi: 10.1016/j.resconrec.2025.108435

70. Ghadge A, Er M, Ivanov D, Chaudhuri A. Visualisation of ripple effect in supply chains under long-term, simultaneous disruptions: a system dynamics approach. *Int J Prod Res*. 2022;60(20):6173-6186.

doi: 10.1080/00207543.2021.1987547

71. Yang Z, Song Z, Liu W. Risks and crisis propagation in global palladium trade network: Implications for critical resource supply chain security. *J Ind Ecol*. 2025;29(4):1223-1236.

doi: 10.1111/jiec.70038

72. Hu H, Guo S, Qin Y, Lin W. Two-stage stochastic programming model and algorithm for mitigating supply disruption risk on aircraft manufacturing supply chain network design. *Comput Ind Eng*. 2022;175:108880.

doi: 10.1016/j.cie.2022.108880

73. Huang Z, Zhou Y, Lin Y, Zhao Y. Resilience evaluation and enhancing for China's electric vehicle supply chain in the presence of attacks: A complex network analysis approach. *Comput Ind Eng*. 2024;195:110416.

doi: 10.1016/j.cie.2024.110416

74. Zhang L, Su W, Liao S, Wang S. Enhancing energy security through multi-scale network analysis: Robustness in global crude oil shipping-trade networks. *Reliab Eng Syst Saf*. 2025;265:111525.

doi: 10.1016/j.ress.2025.111525

75. Tian W, Huang X, Shao L, Wang Z, Li Y. Assessment and evolution analysis of the global wood pulp trade network resilience based on underload cascading failure. *J Clean Prod*. 2025;518:145742.

doi: 10.1016/j.jclepro.2025.145742

76. Dash A, Sarmah S, Tiwari M, Jena SK, Glock CH. Cybersecurity investments in supply chains with two-stage risk propagation. *Comput Ind Eng*. 2024;197:110519.

doi: 10.1016/j.cie.2024.110519

77. Xiao R, Xiao T, Zhao P, Zhang M, Ma T, Qiu S. Structure and resilience changes of global liquefied natural gas shipping

network during the Russia-Ukraine conflict. *Ocean Coast Manag*. 2024;252:107102.

doi: 10.1016/j.ocecoaman.2024.107102

78. Hou B, Wang X, Tang J. Identifying critical node set in supply chain network considering hybrid operational risk management. *Int J Prod Econ*. 2025;291:109864.

doi: 10.1016/j.ijpe.2025.109864

79. Vaid R, Jain K, Sahi GK, *et al*. Designing a resilient agriculture supply network for mitigating the disruptions. *Ann Oper Res*. 2025;344(1):313-343.

doi: 10.1007/s10479-024-06143-w

80. Lavassani KM, Boyd ZM, Movahedi B, Vasquez J. Ten-tier and multi-scale supply chain network analysis of medical equipment: random failure & intelligent attack analysis. *Int J Prod Res*. 2023;61(24):8468-8492.

doi: 10.1080/00207543.2022.2152892

81. Artime O, Grassia M, De Domenico M, *et al*. Robustness and resilience of complex networks. *Nat Rev Phys*. 2024;6(2):114-131.

doi: 10.1038/s42254-023-00676-y

82. Zhao H, Bu H, Li Z. Resilience analysis and enhancement strategies of leader-driven automotive supply chain based on complex network. *Int J Gen Syst*. 2025;54(5):1-29.

doi: 10.1080/03081079.2025.2590647

83. Massari GF, Giannoccaro I. The importance of the structural pattern for the resilience of circular economy networks: A network-based approach. *J Clean Prod*. 2024;436:140164.

doi: 10.1016/j.jclepro.2023.140164

84. Wang W, Karimi F, Khalilpour K, Green D, Varvarigos M. Robustness analysis of electricity networks against failure or attack: The case of the Australian National Electricity Market (NEM). *Int J Crit Infrastruct Prot*. 2023;41:100600.

doi: 10.1016/j.ijcip.2023.100600

85. Negahban A, Smith JS. A joint analysis of production and seeding strategies for new products: an agent-based simulation approach. *Ann Oper Res*. 2018;268(1-2):41-62.

doi: 10.1007/s10479-016-2389-8

86. Fu X, Xu X, Li W. Cascading failure resilience analysis and recovery of automotive manufacturing supply chain networks considering enterprise roles. *Physica A*. 2024;634:129478.

doi: 10.1016/j.physa.2023.129478