

Article

From Supply Chains to Interdependent Logistics Infrastructure: Topological Fragility, Shock Amplification and Orbital Computing

Klavdij Logožar 

Faculty of Economics and Business, University of Maribor, 2000 Maribor, Slovenia; klavdij.logozar@um.si

Abstract

Background: High-technology supply chains are interdependent logistics infrastructures in which digital, energy, manufacturing, cloud and orbital layers are tightly coupled. This paper examines how such layering changes supply chain resilience and systemic vulnerability. **Methods:** The paper develops an analytical–conceptual framework linking supply chain resilience, interdependent infrastructure theory and network topology. It introduces Topological Phase Vulnerability (TPV), capturing proximity to structural fragility thresholds, and the Shock Amplification Coefficient (SAC), conceptualizing disruption amplification as a function of centrality concentration, cross-layer coupling and reconfiguration capacity. The framework is supported by a fuzzy-inspired diagnostic scorecard and stylized assessment of alternative infrastructure configurations. Orbital computing is an extreme illustrative context because it combines dependence on advanced semiconductor fabrication, hyperscale cloud orchestration, energy systems, launch capacity and logistics coordination. **Results:** Highly centralized configurations are more likely to transform local disruptions into cross-layer cascades, whereas modular and distributed configurations are more likely to contain disruption through redundancy, substitutability and rerouting. **Conclusions:** Resilience in next-generation logistics infrastructure depends not only on capacity or component reliability, but also on topology. Centrality dispersion, modularity and reconfiguration capacity are critical design principles for reducing shock amplification in high-technology supply chains.

Keywords: supply chain resilience; logistics infrastructure; interdependent infrastructures; topological fragility; shock amplification; network centrality; orbital computing; high-technology supply chains; reconfiguration capacity



Received: 24 May 2026

Revised: 22 June 2026

Accepted: 29 June 2026

Published: 1 July 2026

Copyright: © 2026 by the author.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

High-technology supply chains and logistics infrastructures are entering a new phase of expansion, driven by artificial intelligence (AI), hyperscale data systems, advanced semiconductor fabrication, energy-intensive computing and emerging orbital or space-enabled infrastructures. From a logistics and supply chain resilience perspective, this expansion raises a specific problem: can increasingly interdependent logistics infrastructures absorb, reroute and recover from disruption when critical functions are concentrated in highly central nodes and tightly coupled layers?

In this paper, orbital computing refers to the use of space-based or orbital assets to support data-intensive computing, processing, storage or orchestration functions usually associated with terrestrial cloud and high-performance computing infrastructures. It is not

treated as an independent domain of space technology. Rather, it is used as an extreme illustrative context in which orbital assets, launch and servicing capacity, ground segments, terrestrial cloud orchestration, energy infrastructure and advanced semiconductor supply become mutually dependent. Its analytical value lies in making visible a broader logistics problem: additional infrastructure layers may increase capability while also creating new pathways for disruption.

Contemporary logistics and supply chain systems have often been designed around normal-time optimization: cost minimization, just-in-time coordination, capacity utilization and centralization around dominant nodes. Supply chain resilience research has long warned that efficiency-oriented designs can reduce redundancy and increase vulnerability to disruption [1]. More recent reviews show that the propagation of disruptions, recovery strategies, and resilience capabilities remain central concerns in the field [2,3]. Research on interdependent infrastructures adds a different warning: system-level resilience cannot be inferred from the performance of individual components when infrastructure layers are functionally dependent [4]. Modelling work on critical infrastructure interdependence further shows that the direction of dependency, propagation channels, and recovery options shape system vulnerability [5,6]. Rinaldi et al. [7] show why such dependence must be analyzed across physical, cyber, geographic and logical interdependencies rather than within isolated infrastructure systems. Network research makes the same point from a topological angle: the robustness and resilience of complex networks depend on where disruption occurs and how connectivity is organized [8]. Highly centralized networks may be robust to random variation but vulnerable to targeted disruption of high-connectivity or high-load nodes [9,10]. In coupled networks, failures can become nonlinear when disruption in one layer reduces functionality in another [11,12].

This paper does not treat orbital computing primarily as a question of technological feasibility or as a socio-technical transition problem. The focus is narrower: how logistics infrastructure topology shapes the translation of localized disruption into system-wide disturbance, recovery demand and reconfiguration pressure. Geopolitical pressure matters because it can alter access to strategic inputs and infrastructure chokepoints [13]. Semiconductor industrial policy matters because it directly targets the location and concentration of advanced fabrication capacity [14]. Techno-national restructuring matters because it can reduce substitutability across regions, platforms and infrastructure blocs [15]. The core issue, however, is not geopolitics as such. It is how external pressures interact with centrality concentration, cross-layer coupling and limited reconfiguration capacity.

Despite major advances in supply chain resilience, interdependent infrastructure modelling, and complex network analysis, there remains a need for a logistics-oriented framework that connects these mechanisms. Existing work explains resilience capabilities, cascading effects, network robustness and infrastructure interdependence. Less attention has been paid to how these insights can be organized into a supply chain and logistics resilience framework for emerging high-technology infrastructures whose critical layers span semiconductor fabrication, hyperscale cloud control, energy systems, launch logistics and orbital assets.

The paper addresses this gap by conceptualizing high-technology supply chains as interdependent logistics infrastructures. It introduces two constructs. Topological Phase Vulnerability (TPV) refers to the proximity of an infrastructure configuration to a structural fragility threshold at which disruption in high-centrality nodes can trigger disproportionate system effects. Shock Amplification Coefficient (SAC) refers to the conditional amplification potential of a local disruption as it moves across layers, shaped by centrality concentration, cross-layer coupling and reconfiguration capacity. The aim is not to offer calibrated numer-

ical indicators, but to provide a diagnostic framework for analyzing when local disruption is likely to remain contained and when it may become systemic.

The paper makes three contributions to logistics and supply chain resilience research. First, it conceptualizes centrality concentration as a logistics resilience bottleneck, showing why high throughput, visibility and coordination efficiency may coexist with hidden systemic vulnerability. Second, it distinguishes between pre-shock structural vulnerability and post-shock amplification by developing TPV and SAC as analytically distinct yet related constructs. Third, it uses orbital computing as an extreme illustrative context to show how new infrastructure layers can either buffer disruption or deepen dependence on existing bottleneck nodes, depending on whether they increase substitutability, modularity and reconfiguration capacity.

The remainder of the paper proceeds as follows. Sections 2 and 3 present the theoretical background and methodological approach. Sections 4 and 5 develop the framework by linking interdependent logistics infrastructure, centrality concentration and shock amplification. Section 6 discusses resilience-oriented reconfiguration and alternative infrastructure configurations, while Sections 7 and 8 present the discussion and conclusion.

2. Theoretical Background and Research Gap

Research on supply chain and logistics resilience has moved beyond viewing disruption as an exceptional interruption to otherwise stable flows. In contemporary logistics systems, disruption is also shaped by network design: where capacity is concentrated, how layers depend on one another, which nodes become unavoidable and how quickly flows can be redirected when a strategic node fails. This matters for high-technology logistics infrastructures because semiconductor fabrication, hyperscale cloud facilities, energy systems, launch logistics and orbital computing increasingly form an operational stack in which physical movement, digital coordination and infrastructure ownership are difficult to separate.

Several literature streams help analyze this problem. Supply chain resilience research explains the role of flexibility, redundancy, visibility, collaboration and recovery capabilities. Ripple-effect and disruption-propagation studies examine how disruptions travel across supply chain structures. Digital and platform logistics research shows how logistics control becomes embedded in data infrastructures, platform governance and ownership arrangements. Critical infrastructure and complex-network research provide concepts for interdependencies, cascading failures and central nodes. Yet these streams do not fully explain how efficient, centralized and tightly coupled logistics infrastructures can cross a structural threshold at which a localized shock becomes systemically amplified.

This paper brings these streams together through two constructs. TPV refers to the proximity of a logistics infrastructure configuration to a structural vulnerability threshold. SAC refers to the extent to which a local disruption is enlarged by node centrality, cross-layer dependence and limited reconfiguration capacity. The aim is not to replace established resilience concepts, but to provide a logistics-oriented vocabulary for configuration-based fragility in infrastructure systems whose failure pathways are no longer confined to a single firm, tier or transport mode.

2.1. Supply Chain and Logistics Resilience: Capabilities, Recovery and Structural Limits

The supply chain resilience literature provides the most direct starting point. Christopher and Peck [16] framed resilience as a supply chain design and management problem rather than merely a business continuity issue. Their work remains important because it shifted attention from local risk prevention to supply chain-wide vulnerability. Ponomarev and Holcomb [17] further conceptualized resilience as adaptive capability: the ability to

prepare for unexpected events, respond to disruptions and recover while maintaining continuity of operations. Pettit et al. [18] advanced this logic by linking vulnerabilities and capabilities within a structured framework, which was later extended into a resilience assessment and management approach [19]. These contributions established the core managerial language of resilience: flexibility, redundancy, collaboration, visibility, adaptability and recovery.

Several reviews have clarified the scope and limits of this literature. Tukamuhabwa et al. [1] showed that supply chain resilience research is theoretically diverse yet often fragmented across definitions, strategies, and empirical settings. Katsaliaki et al. [2] mapped the disruption and resilience literature and showed that studies predominantly focused on disruption types, mitigation strategies, and performance effects. Wieland and Durach [20] added a useful distinction between engineering-oriented and social-ecological perspectives on resilience. The former tends to emphasize return to a prior state; the latter stresses adaptation and transformation. For the present paper, that distinction is central. High-technology logistics infrastructures may not simply need to “bounce back”. In some configurations, the pre-shock structure is itself the source of fragility.

Quantitative resilience research has also become more sophisticated. Hosseini et al. [21] review models that measure resilience capacity, disruption response and recovery behaviour. Hosseini et al. [22] argue for an open-system view of supply chain resilience, in which the system interacts with its environment and cannot be understood solely by restoring internal performance. These approaches are useful because they make resilience more measurable. Still, many resilience metrics remain capability- or performance-oriented. They ask whether a supply chain can absorb, adapt or recover. They ask less often whether the system’s topology has moved close to a threshold where a small targeted disruption can trigger disproportionate cross-layer consequences.

That gap is not a criticism of resilience theory. It is a sign that the empirical object has changed. In high-technology logistics infrastructures, resilience depends not only on whether firms hold buffers, collaborate or monitor risk. It also depends on whether critical logistics, energy, data and production layers have become concentrated around a small number of mutually dependent nodes. A semiconductor fabrication facility, a hyperscale cloud region, an energy corridor or a launch provider may each appear manageable when analyzed separately. The logistics risk emerges when these nodes become co-dependent within the same infrastructure configuration.

2.2. Disruption Propagation, Ripple Effects and Resilient Network Design

The second relevant stream examines the propagation of disruption. Ivanov et al. [23] developed the ripple-effect perspective to analyze how disruption spreads through supply chains and affects performance beyond the initially disrupted node. Dolgui et al. [24] later distinguished the ripple effect from the bullwhip effect: the bullwhip effect concerns demand-signal distortion, whereas the ripple effect concerns disruption-driven structural and performance impacts across the supply chain. This distinction is important for the present argument. Shock amplification in logistics infrastructure is not simply volatility moving upstream or downstream. It is the enlargement of a local failure through structural dependence.

Work on resilient supply chain network design has translated this concern into optimization and design problems. Maharjan and Kato [25] review studies that use network design models to enhance resilience to disruptions. These models typically evaluate facility location, sourcing redundancy, backup capacity, rerouting and recovery decisions. They are analytically stronger than generic resilience discussions because they force the analyst to specify nodes, arcs, capacities and disruption scenarios. They also show that resilience

is costly: redundancy, flexibility and alternative routing require prior investment, not just managerial intent.

Yet resilient network design usually operates inside a bounded supply chain or logistics network. The decision problem is often formulated around facilities, suppliers, distribution centres, transport links or demand zones. That is appropriate for many logistics problems, but less adequate for infrastructures where the relevant dependency chain crosses sectoral layers. A disruption in semiconductor fabrication can constrain cloud hardware expansion; cloud constraints can affect logistics visibility and optimization; energy scarcity can limit both data-centre operation and manufacturing; launch bottlenecks can restrict the deployment or replacement of orbital assets. These are not merely longer supply chains. They are interdependent logistics infrastructures.

Recent viability-oriented work helps to widen the frame. Ivanov [26] conceptualizes the viable supply chain as a system that can maintain itself under changing conditions by integrating agility, resilience, and sustainability. Ivanov et al. [27] extend this reasoning towards viable ecosystems, which is closer to the infrastructure problem addressed here. Viability is useful because it shifts attention from recovery after a known disruption to survival under long-term instability. However, even viability research does not yet give logistics scholars a concise way to describe when a network configuration becomes topologically fragile. TPV and SAC are introduced to make that condition more visible.

2.3. Digital Logistics, Platform Control and Infrastructure Ownership

Digital logistics research adds a different angle. Logistics systems are no longer coordinated only through physical assets, contracts and transport capacity. They are increasingly governed through data infrastructures, platforms, algorithms, cloud services and real-time visibility systems. This changes the meaning of logistics control. The actor that owns or governs the digital layer may influence routing, prioritization, service quality, customer access and exception management even without owning every physical asset.

The Physical Internet literature anticipated part of this shift by imagining logistics as an open, interconnected system of shared facilities and transport resources. Yang et al. [28], for example, examine vendor-managed inventory in an interconnected logistics service environment, where users can exploit shared storage and multisourcing options. Such work shows the resilience potential of modular and open logistics networks. If logistics resources are genuinely substitutable and interoperable, disruption in one location need not paralyze the whole system.

Platform logistics complicates this optimistic view. Online platforms may rely on third-party logistics, develop self-built logistics, or combine platform-controlled warehousing, delivery and data systems. Yu et al. [29] ask whether it is always advantageous for online platforms to establish in-house logistics in a competitive retail setting. Their analysis is useful here not because it studies TPV or orbital computing directly, but because it shows that logistics ownership is a strategic control decision. Self-built logistics can improve service control and differentiation, yet they may also increase fixed commitments and deepen dependence on a platform-specific infrastructure. For this paper, the point is broader: digital and platform logistics make logistics infrastructure more controllable, but not automatically more resilient.

The same tension appears in hyperscale cloud and AI infrastructure. Centralized cloud regions and data centres provide economies of scale, standardization and advanced coordination capability. They also create shared dependency points for many firms, logistics systems and digital services. In normal operation, centralization can appear to be efficient. Under stress, it can become a route through which disruption is amplified. Logistics research has increasingly focused on digital visibility and platform-enabled coordination,

but has paid less attention to the fragility that arises when digital logistics depends on concentrated cloud, energy, and semiconductor infrastructure.

2.4. Interdependent Infrastructures and Network Topology

Critical infrastructure research provides a more direct language for interdependency. Rinaldi et al. [7] distinguish between physical, cyber, geographic, and logical interdependencies among infrastructures. Their framework is valuable because it prevents a narrow view of infrastructure failure. A logistics system may be disrupted because a physical input is unavailable, a cyber system fails, geographically co-located assets are affected by the same event, or institutional and operational rules transmit the consequences of disruption. Ouyang [6] reviews modelling and simulation approaches for interdependent critical infrastructures and shows that interdependency analysis requires attention to multiple systems, not only to individual asset reliability.

Complex-network research provides sharper topological insights. Albert et al. [30] showed that some complex networks are robust to random failures but vulnerable to targeted attacks on highly connected nodes. Motter and Lai [31] demonstrated how attacks on overloaded or highly loaded nodes can trigger cascading failures. Buldyrev et al. [11] showed that interdependent networks may behave differently from isolated networks: coupling can make systems more fragile, not more robust, when failures propagate across dependent layers. These findings are not logistics theories in the narrow sense, but they are highly relevant for logistics infrastructures that increasingly depend on a few critical nodes, hubs and platforms.

The risk in this paper is the casual importation of network language. Terms such as “topological fragility” can sound metaphorical if they are not anchored in logistics mechanisms. For that reason, TPV is used here in a deliberately restricted sense. It does not claim to measure a formal phase transition in the mathematical sense. It denotes a configuration-based vulnerability condition: the more the logistics infrastructure depends on central nodes, the tighter the layer coupling, and the poorer the substitutability, the closer it is to a threshold at which local disruption can produce non-local consequences. SAC then captures the amplification side of the same problem. It asks not only whether a node is critical, but also how strongly disruption at that node is likely to propagate through the rest of the infrastructure.

This framing also clarifies the difference between ordinary disruption propagation and shock amplification. Propagation refers to the movement of disruption across connected elements. Amplification refers to a change in scale: the resulting system impact becomes larger than the initial disturbance would suggest. A port strike, a semiconductor capacity shortage, a cloud region outage, or a launch bottleneck may each propagate through connected supply chains. They become amplification problems when the affected node is central, when several operational layers depend on it simultaneously, and when reconfiguration options are limited or slow.

2.5. Space Logistics and Orbital Computing as an Extreme Logistics Context

Space and orbital computing are used in this paper as an extreme illustrative context, not as the only or even the most mature empirical domain. The point is analytical. Orbital computing makes visible a broader logistics transformation already underway on Earth: compute capacity, energy access, hardware supply, launch capacity, data routing, and operational resilience are becoming part of the same infrastructure problem.

Space logistics research has developed around launch scheduling, in-space servicing, assembly, maintenance, refuelling and orbital supply chains. Ho [32] reviews space logistics modelling and optimization, including in-space servicing, assembly and manufacturing.

This literature is important because it treats space not only as an engineering domain but as a logistics system with flows, capacities, maintenance needs and resource constraints. As satellite constellations, orbital servicing and space-based data-processing concepts develop, orbital infrastructure becomes a useful boundary case for logistics theory.

The paper does not assume that large-scale orbital computing is already operational or economically proven. On the contrary, its value for the argument lies partly in its unresolved status. Orbital computing exposes the logistical consequences of pushing digital infrastructure into a more constrained environment: launch capacity is limited, repair is difficult, hardware replacement cycles are slower, orbital slots and communications links matter, and energy, thermal management, and radiation tolerance become logistical constraints rather than background engineering details. In such a setting, centrality and coupling are not abstract properties. They determine whether the system can absorb failure, reroute service, replace capacity or remain trapped by a bottleneck.

Orbital computing, therefore, serves as a stress case for the wider concept of interdependent logistics infrastructure. The same analytical logic can apply to terrestrial semiconductor–cloud–energy systems, advanced manufacturing clusters, strategic ports, or AI-enabled logistics platforms. The contribution does not depend on predicting the future of orbital data centres. It depends on showing how logistics resilience changes when the infrastructure supporting digital coordination becomes a critical logistics layer in its own right.

2.6. Research Gap and Positioning of the Paper

The reviewed literature leaves three specific gaps. First, supply chain resilience research explains capabilities and recovery strategies well, but it less often specifies when the structure of the logistics infrastructure itself becomes the source of vulnerability. Flexibility, redundancy and visibility remain necessary, but they do not fully explain why highly capable systems can still fail disproportionately when a central infrastructure layer is disrupted.

Second, research on ripple effects and resilient network design provides tools for modelling disruption propagation and network redesign, but most studies remain bounded to supply chain or logistics networks. High-technology logistics infrastructure is increasingly cutting across the production, energy, digital, launch, and orbital layers. The relevant disruption pathway may therefore move across sectors before returning as a logistics failure.

Third, critical infrastructure and complex network research explains interdependencies, cascading failures, and centrality-based vulnerability, but these insights have not been fully translated into logistics and supply chain resilience concepts. Logistics scholars need a vocabulary that remains close to operational realities: capacity concentration, routing alternatives, platform dependence, infrastructure ownership, reconfiguration time and cross-layer coupling.

The paper addresses these gaps by conceptualizing high-technology supply chains as interdependent logistics infrastructures. It introduces TPV to describe a configuration's proximity to a structural vulnerability threshold and SAC to describe the potential for local shocks to be amplified across layers. Table 1 summarizes how the paper builds on, but also departs from, the main literature streams.

The resulting contribution is deliberately conceptual but not merely speculative. The framework draws on established research on resilience, disruption propagation, digital logistics, and infrastructure interdependency, then narrows its focus to a specific under-developed mechanism: shock amplification arising from the topology of interdependent logistics infrastructures. The next section explains how the framework was developed and how the stylised assessment should be read.

Table 1. Existing approaches to resilience in logistics and infrastructure networks, and the gap addressed by this paper.

Literature Stream	What It Explains	Remaining Limitation	Role in This Paper
Supply chain and logistics resilience	Capabilities such as preparedness, recovery, flexibility, redundancy and adaptability	Strong on capabilities, weaker on when infrastructure configuration itself becomes fragile	Reframes resilience as partly configuration-dependent
Ripple effect and disruption propagation	How disruptions spread across supply chain tiers and affect performance	Often focuses on propagation within bounded supply chain structures	Distinguishes propagation from cross-layer amplification
Resilient supply chain network design	Facility location, backup sourcing, redundancy, rerouting and recovery choices	Usually assumes a defined logistics or supply chain network	Extends the design problem to interdependent logistics infrastructures
Digital and platform logistics	Visibility, platform control, data-driven coordination and logistics ownership	Less attention to dependence on concentrated cloud, data, energy and platform infrastructures	Links digital control to infrastructure fragility
Interdependent critical infrastructure	Cascading effects across physical, cyber, geographic and logical dependencies	Developed mostly outside logistics and SCM	Translates interdependency into logistics terms: substitutability, coupling and reconfiguration
Complex networks and space logistics	Centrality, cascading failure, attack vulnerability and orbital infrastructure constraints	Topology concepts risk becoming metaphorical if not grounded in logistics	Uses topology cautiously and treats orbital computing as an extreme illustrative context

Source: Author's own compilation based on the reviewed literature.

3. Methodological Approach: Conceptual Framework Development and Illustrative Assessment

This paper employs an analytical–conceptual research design, supported by a diagnostic, illustrative assessment. The aim is not to estimate the probability of infrastructure failure, nor to calibrate a simulation model against observed disruption data. The aim is to develop a logistics resilience framework to analyze how localized shocks may be systemically amplified when high-technology logistics infrastructure is centralized, tightly coupled, and difficult to reconfigure.

The methodological choice follows from the character of the phenomenon. Semiconductor fabrication, hyperscale cloud, energy infrastructure, launch logistics and orbital computing are increasingly connected, but the empirical record of their joint disruption behaviour remains incomplete. A large-sample empirical design would require comparable observations across infrastructure layers that are still unevenly documented. A calibrated simulation would require assumptions about interdependencies, substitution possibilities and recovery times that are not yet standardized across domains. Treating the article as if it were an empirical validation study would therefore be misleading. The more appropriate task at this stage is to define the problem, specify the constructs and provide a transparent diagnostic logic that future empirical work can operationalize.

Conceptual articles can contribute when they clarify an emerging phenomenon, develop new constructs, connect previously separate studies or specify relationships that later empirical work can test [33,34]. This paper follows that logic. It does not present TPV

and SAC as already validated metrics. It introduces them as logistics-oriented constructs for analyzing configuration-based fragility in interdependent infrastructure systems. The paper introduces two methodological devices: a fuzzy-inspired diagnostic scorecard and a structured focused comparison of stylized infrastructure configurations.

3.1. Research Design and Unit of Analysis

The article is positioned as a conceptual framework paper with an illustrative diagnostic component. The framework is developed from research on supply chain resilience, disruption propagation, ripple effects, resilient network design, digital logistics, platform logistics, interdependent critical infrastructure and complex networks. These streams are not treated as parallel bodies of literature to be summarized mechanically. They are used to isolate a specific logistics problem that remains underdeveloped: the possibility that the same infrastructure topology that creates efficiency under normal conditions can amplify shocks under stress.

The unit of analysis is the interdependent configuration of logistics infrastructure. This is broader than a firm, dyadic buyer–supplier relationship, a transport corridor, or a single supply chain. It refers to a configuration of infrastructure layers, nodes and dependencies through which physical logistics, digital coordination, production capacity, energy access and space-enabled or orbital assets may interact.

This choice is deliberate. In high-technology logistics systems, disruption does not necessarily remain inside the layer where it begins. A shortage in advanced chips may constrain cloud expansion; a cloud outage may disrupt logistics visibility and decision systems; energy scarcity may affect fabrication plants and data centres at the same time; launch bottlenecks may delay the replacement of orbital assets. The relevant logistics vulnerability is therefore not only within-layer disruption, but cross-layer amplification.

Table 2 summarizes the paper’s methodological logic.

Table 2. Methodological procedure used to develop and apply the conceptual framework.

Step	Purpose	Analytical Procedure	Output in This Paper
1. Problem framing	Identify the unresolved logistics resilience problem	Synthesis of resilience, ripple-effect, digital logistics, infrastructure-interdependency and network-fragility research	Shock amplification in interdependent logistics infrastructures
2. Unit of analysis	Move beyond firm-level, dyadic or single-chain analysis	Definition of the interdependent logistics infrastructure configuration	Infrastructure configuration treated as a system of nodes, layers and dependencies
3. Construct development	Translate the gap into logistics-oriented concepts	Abductive derivation of TPV and SAC from recurring mechanisms in the reviewed literature	Topological Phase Vulnerability and Shock Amplification Coefficient
4. Diagnostic assessment	Turn the constructs into an assessable framework	Use of centrality concentration, cross-layer coupling and reconfiguration capacity as diagnostic dimensions	Fuzzy-inspired scorecard and structured focused comparison
5. Boundary conditions	Prevent overgeneralization and prepare future empirical work	Clarification of scope, limits and operationalization routes	Future pathways for simulation, multiplex modelling, case comparison and sensitivity analysis

Source: Author’s compilation.

3.2. Construct Development and Diagnostic Dimensions

The two constructs proposed in this article respond to a limitation in existing resilience language. Supply chain resilience research is strong at describing capabilities such as redundancy, flexibility, visibility, collaboration, adaptability and recovery. Disruption-propagation research explains how failures travel through supply chain structures. Critical infrastructure and complex-network studies explain interdependencies and cascading effects. What remains less developed is a logistics-centred vocabulary for describing when a high-performing infrastructure configuration approaches an amplification threshold.

TPV describes this pre-disruption condition. It refers to the proximity of a logistics infrastructure configuration to a structural vulnerability threshold. “Topological” is used here in a restricted logistics sense: it refers to the arrangement of critical nodes, dependencies and reconfiguration pathways. The paper does not claim to measure a formal mathematical phase transition. TPV is a diagnostic construct that assesses whether infrastructure design is moving closer to or further from a fragility threshold.

SAC refers to the potential for a local disruption to produce a disproportionate system-level effect. It is not presented as a calibrated numerical coefficient in this paper. A disruption at a peripheral, substitutable node may propagate, but it is unlikely to trigger large-scale amplification. A disruption at a central node that connects several layers and has limited substitutes is more likely to produce a system-wide effect.

The distinction is temporal and functional. TPV describes the structural condition before a shock. SAC describes the potential for conditional amplification following a shock. TPV asks how close the configuration is to a fragility threshold. SAC asks how strongly the impact could be enlarged if a disruption affects a critical point.

The diagnostic framework is built around three dimensions:

- Centrality concentration, or the extent to which critical logistics, digital, production or infrastructure functions depend on a small number of nodes.
- Cross-layer coupling, or the extent to which disruptions in one layer affect other layers.
- Reconfiguration capacity, or the ability to reroute, substitute, decentralize, repair or otherwise reorganize flows and functions after disruption.

Centrality is not inherently inefficient or fragile. It may create scale economies, standardization, faster coordination and clearer investment focus. Its resilience implication depends on substitutability and containment. Cross-layer coupling matters because weak coupling allows problems to remain local, whereas tight coupling allows failures to move from energy to cloud, from cloud to logistics visibility, from semiconductor supply to AI infrastructure, or from launch constraints to orbital service availability. Reconfiguration capacity matters because interdependent logistics infrastructures may require digital, institutional and ownership-level changes, not only transport rerouting.

TPV and SAC are therefore configuration-level properties. They arise from the interaction of centrality, coupling and reconfiguration capacity, not from any single dimension alone.

3.3. Fuzzy-Inspired Diagnostic Map

Figure 1 illustrates the fuzzy-inspired relationship between TPV and SAC [35,36]. Instead of classifying configurations as simply resilient or fragile, it presents six diagnostic profiles based on pre-shock structural vulnerability and conditional shock-amplification potential. The positions are qualitative rather than calibrated: centrality concentration and cross-layer coupling tend to move configurations toward the cascade-prone zone, whereas reconfiguration capacity tends to move them toward containment. The figure does not use numerical membership functions, expert-derived weights, or a formal fuzzy inference system; it offers a disciplined visual language for comparing infrastructure configurations.

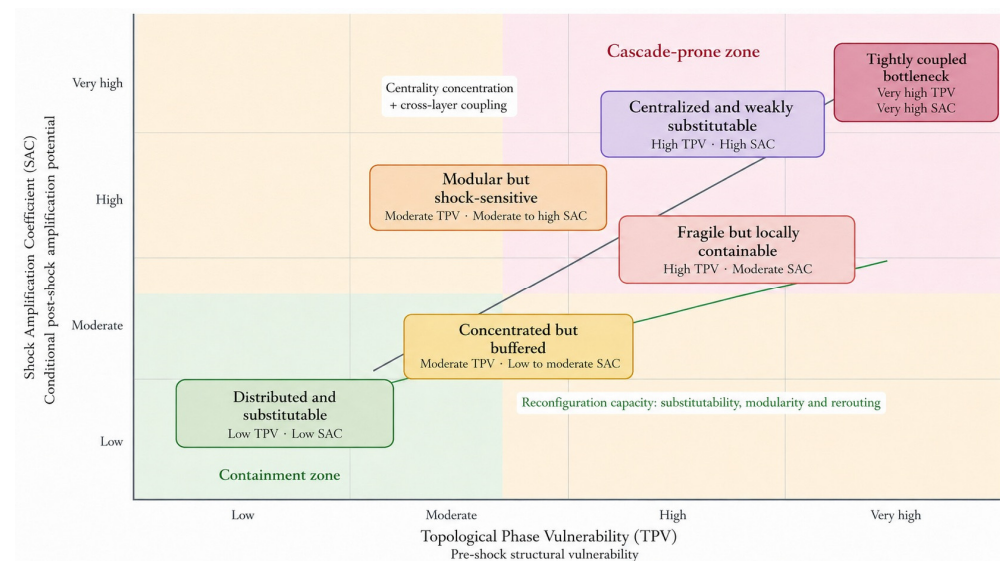


Figure 1. Fuzzy-inspired diagnostic map of Topological Phase Vulnerability and the Shock Amplification Coefficient. Source: Author’s own conceptualization.

TPV and SAC are expected to be related, but they are not identical. A configuration may display high TPV because it is centralized and weakly substitutable, while SAC remains moderate if cross-layer interfaces contain the disruption. Conversely, a configuration with only moderate TPV may exhibit a high SAC if a targeted shock affects a node that connects otherwise separable layers. This distinction is important because propagation and amplification are not the same. Propagation means that the disruption moves across connected elements. Amplification means the resulting impact exceeds what the initial disturbance would suggest.

3.4. Structured Focused Comparison

The second methodological device is a structured focused comparison [37]. This approach applies the same analytical questions across multiple cases or configurations to avoid anecdotal comparison. In this article, the objects of comparison are stylized logistics infrastructure configurations rather than fully developed empirical case studies. The comparison is “structured” because each configuration is assessed using the same questions, and “focused” because the questions address only the mechanisms relevant to TPV and SAC.

The four configurations are stylized because real logistics infrastructures are hybrid. A platform may use centralized cloud infrastructure, distributed warehouses, outsourced last-mile carriers and satellite-enabled visibility at the same time. A semiconductor supply chain may combine geographic concentration in fabrication with distributed downstream assembly and testing. A space-enabled logistics system may depend simultaneously on terrestrial cloud services, ground stations, launch capacity and orbital assets. Stylized configurations therefore isolate mechanisms rather than represent clean empirical types.

The paper compares four stylized configurations:

- Centralized configuration: critical functions are concentrated in a small number of high-capacity nodes.
- Modularized configuration: functions are separated into partly substitutable modules with clearer interfaces.
- Distributed configuration: capacity and control are spread across multiple nodes and locations.

- Orbital-hybrid configuration: terrestrial and orbital or space-enabled layers are combined, resulting in constrained reconfiguration and stronger cross-layer dependencies.

Table 3 presents the comparison protocol.

Table 3. Structured focused comparison protocol for infrastructure configurations.

Diagnostic Question	Analytical Purpose	Link to TPV/SAC
Which nodes or layers perform unavoidable functions?	Identifies critical concentration points	High concentration increases TPV
Are critical nodes substitutable, and under what time horizon?	Distinguishes formal alternatives from operationally usable alternatives	Low substitutability increases TPV and SAC
Which layers depend on the same node, provider, platform or energy source?	Identifies cross-layer coupling	Strong coupling increases amplification potential
Can disruption be contained within one layer, or is cross-layer transmission likely?	Separates propagation from systemic amplification	Cross-layer transmission increases SAC
Who has the authority and capability to reconfigure the system?	Links technical reconfiguration to governance and ownership	Weak authority reduces reconfiguration capacity
Does the configuration trade normal-time efficiency for stress-time fragility?	Identifies the core logistics resilience trade-off	Efficiency–fragility trade-offs help interpret TPV and SAC

Source: Author's compilation.

The same protocol is applied to each stylized configuration. This gives the assessment a consistent structure and makes the logic contestable: disagreement can be located in centrality, coupling, substitutability, reconfiguration speed or governance authority.

3.5. Application, Limits and Future Operationalization

The diagnostic assessment proceeds in two stages. First, each configuration is assessed against centrality concentration, cross-layer coupling and reconfiguration capacity. Second, the configuration is interpreted in terms of expected TPV and SAC. The purpose is not to produce a league table of configurations, but to identify vulnerability profiles.

A centralized configuration may be efficient in normal conditions because it supports scale economies, standardized governance and concentrated expertise. Its vulnerability emerges when the central node is difficult to bypass. A modularized configuration can reduce TPV by creating clearer boundaries between functions, although this depends on whether interfaces are genuinely interoperable rather than only nominally modular. A distributed configuration can reduce single-node dependency, but it may also increase coordination complexity, cyber exposure and governance fragmentation. An orbital-hybrid configuration is included as an extreme context in which launch capacity, orbital replacement, in-space servicing, communications links, ground stations and energy or thermal constraints make reconfiguration particularly difficult.

The illustrative assessment is not empirical validation. It does not show that TPV or SAC have been measured in observed systems. It demonstrates how the proposed constructs can be applied analytically and distinguish pre-shock structural vulnerability from conditional amplification potential. This distinction is central to the article's contribution.

The framework is most relevant for logistics systems in which several infrastructure layers interact, such as semiconductor logistics, cloud-dependent logistics platforms, AI-enabled fulfilment systems, energy-intensive digital infrastructure, strategic transport hubs, launch logistics and emerging space-enabled services. It is less useful for simple, local or weakly digitized logistics systems where disruption remains confined to a single warehouse, supplier or transport link.

The framework has four limits. First, it does not estimate the probability of disruption; TPV describes structural exposure, not event likelihood. Second, it does not claim that centralization is inherently bad; the risk arises when centralization coincides with tight coupling and weak reconfiguration capacity. Third, it does not assume that distributed systems are inherently resilient; distribution may reduce single-node exposure while increasing coordination complexity. Fourth, the scorecard is not a substitute for empirical testing; its categories are qualitative and diagnostic rather than calibrated measures.

Future studies could operationalize the framework through multiplex network modelling, simulation, dependency-matrix analysis, comparative case studies, AHP–BN risk assessment or sensitivity analysis. These methods could translate centrality concentration into network measures, cross-layer coupling into dependency structures and reconfiguration capacity into recovery times, spare capacity, substitutability ratios or governance constraints. The contribution of the present article is the prior conceptual step: defining the logistics problem, developing TPV and SAC and providing a diagnostic procedure that can be tested and refined.

Figure 2 summarizes the conceptual logic developed in this section by linking disturbance conditions, interdependent infrastructure layers, centrality concentration, cross-layer coupling, reconfiguration capacity, and the resulting TPV/SAC profile.

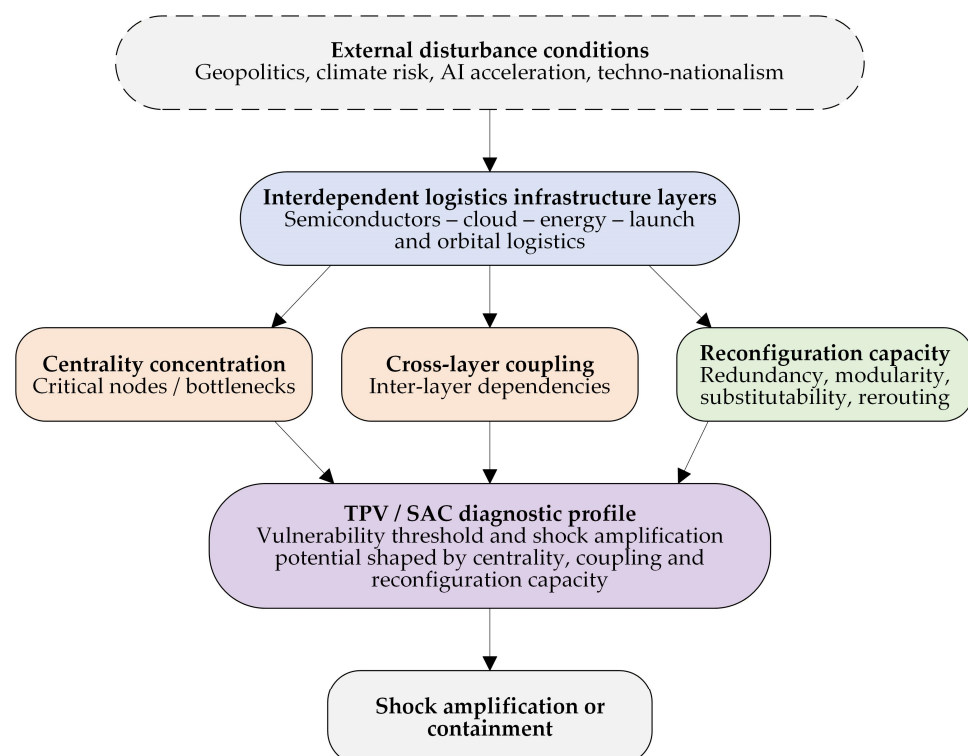


Figure 2. Conceptual framework linking disturbance conditions, infrastructure topology and shock amplification in interdependent logistics infrastructures. Source: Author’s own conceptualization.

4. Interdependent Logistics Infrastructure Architecture and the Centrality Paradox

4.1. Infrastructure Layering and Interdependence

A defining feature of contemporary high-technology systems is that they are not only multi-layered but also functionally dependent across layers. Digital control, energy supply, production capacity, logistics coordination and data-processing infrastructures increasingly operate as a multiplex configuration rather than as separable systems [7]. Studies of interdependent critical infrastructures show that such systems require explicit

attention to functional dependencies, dependency direction, substitute pathways and disruption-propagation channels, rather than the analysis of individual infrastructures in isolation [4–6]. For logistics research, this means that supply chains should increasingly be understood as interdependent logistics infrastructures in which physical, digital, energy and orbital layers jointly shape disruption outcomes.

Research on multiplex networks provides a useful framework for describing this shift. In multilayer energy networks, robustness and resilience depend on how connectivity patterns and critical nodes align across layers, rather than solely on the stability of individual layers [38,39]. Cyber-physical infrastructure studies make the same point operationally: control, monitoring, and mitigation depend on co-modelled electrical and communication layers, which also expand the attack surface and cascade channels [40,41]. For logistics resilience, the issue is therefore architectural: whether inter-layer connections contain disruption or transmit it across the wider system [12,42].

The industrialization of AI shows how this infrastructure stack is intensifying. Frontier AI development depends on hyperscale cloud infrastructure, advanced semiconductor supply and energy-intensive data-centre operations, often controlled by a limited number of dominant providers [43]. This matters for logistics resilience because compute, production and digital control functions become concentrated in a small number of high-load, high-centrality nodes [30,31]. Next-generation digital infrastructures may further intensify this pattern through pervasive sensing, ubiquitous connectivity, and integrated space–air–ground architectures [44].

Orbital computing can be understood as an additional layer within this already expanded stack. It does not replace terrestrial infrastructure; it adds dependencies to it. Orbital compute capacity remains linked to semiconductor fabrication, energy availability, launch capacity, ground segments, cloud orchestration and orbital servicing. A constraint in one layer may therefore alter the operating conditions or recovery options of another. Orbital computing is treated here as an extreme case of logistics infrastructure layering, not as a stand-alone space technology problem.

This escalation produces what can be called infrastructure stratification: loosely connected technology and supply chain systems become layered logistics infrastructures in which performance depends on deep coupling. The resilience problem is that the same coupling also increases dependence on reconfiguration capacity: the ability to reroute demand, substitute functions, activate redundant capacity or decouple affected layers before local degradation becomes systemic.

This structural dynamic links technological concentration with infrastructure-level fragility. As performance concentrates in hyperscale cloud regions, advanced semiconductor fabs, energy hubs and launch providers, peripheral nodes may no longer provide effective buffering or substitution. TPV accumulates as the system approaches thresholds at which the disruption of highly central nodes can trigger disproportionate cascading effects. This is consistent with interdependent infrastructure research showing that vulnerability depends on dependency structures, network parameters and recovery capacity, not only on individual asset performance [45,46].

4.2. Centrality Concentration as a Logistics Resilience Bottleneck

Within this layered architecture, centrality determines where disruption is most likely to matter. Not all nodes contribute equally to logistics resilience. Some nodes carry disproportionate functional load: they coordinate flows, connect sub-networks, concentrate capacity or provide access to otherwise separate layers.

Network research provides the basis for this claim. Entropy-based vulnerability studies show that networks with uneven centrality distributions are more exposed to

targeted disruption [9]. DomiRank centrality similarly identifies locally dominant nodes whose removal can cause substantial degradation [10]. This is consistent with classical complex-network findings: heterogeneous networks may tolerate random failures, but remain vulnerable when highly connected or high-load nodes are disrupted [30,31]. For logistics, the implication is direct: aggregate redundancy does not guarantee resilience if control, routing or capacity is concentrated in a few dominant nodes.

This problem becomes more severe in interdependent systems. General research on complex-network robustness shows that resilience depends on where disruption occurs, not only on how many nodes or links fail [8]. Buldyrev et al. [11] show that interdependent networks can experience catastrophic cascades when failures in one layer reduce functionality in another. Cascading-failure research further indicates that such processes may become non-linear under specific dependency and load conditions [12]. Fu et al. [42] note that vulnerability analysis in interdependent networks must also consider strategies to limit cascade transmission. In multiplex logistics infrastructures, dominant nodes can therefore become bridges between otherwise separable substructures. Their disruption shifts the problem from local degradation to a cross-layer cascade.

Contemporary high-technology supply chains clearly show this pattern. Advanced semiconductor fabrication is spatially and technologically concentrated, with leading-edge capacity located in a small number of facilities and regions [14]. Hyperscale cloud infrastructure is similarly dominated by a few providers that control compute, data and platform ecosystems [43]. Industrial policy responses such as the US CHIPS and Science Act acknowledge these chokepoints by treating semiconductor supply as a strategic domain shaped by techno-national competition [13]. For logistics resilience analysis, the important point is the overlap between industrial concentration and topological centrality: the same facilities, firms and platforms that enable scale may also amplify disruption.

The centrality paradox follows from this overlap. Concentration improves performance under normal conditions. It enables scale economies, standardization, faster coordination, specialized investment and strategic control. Centralized infrastructures may therefore appear more robust because they increase throughput and reduce coordination friction. Yet the same concentration can reduce disruption tolerance: load, control and recovery options become concentrated in structural hubs, and disruption at those hubs may shift the system from local failure to amplified cascade.

Orbital computing intensifies this paradox rather than escaping it. Adding an orbital layer may look like diversification at the macro level, but it may deepen dependence on the same terrestrial bottlenecks: advanced semiconductor fabrication, hyperscale cloud orchestration, energy infrastructure and limited launch capacity. If the orbital layer depends on these already central nodes, it increases cross-layer coupling rather than creating genuine redundancy. The new layer then reinforces, rather than relieves, the centrality of the terrestrial stack.

The centrality paradox, therefore, reframes the resilience problem. The issue is not whether infrastructure is large, advanced or strategically important, but how centrality is distributed across layers and whether alternatives can actually be used during disruption. Dominant nodes become logistics resilience bottlenecks when they maximize efficiency while concentrating recovery dependence. This is where TPV accumulates and where SAC becomes most relevant: local shocks are more likely to be amplified when centrality concentration combines with cross-layer coupling and limited reconfiguration capacity [6,46].

The next section builds on this logic by linking centrality concentration to shock amplification and diagnostic assessment.

5. Shock Amplification and Diagnostic Resilience Assessment

5.1. Shock Amplification and SAC

If the centrality paradox explains why concentrated logistics infrastructures are structurally fragile, SAC addresses the next question: what happens after a shock enters such a configuration? The focus shifts from pre-shock vulnerability to post-shock amplification. Supply chain resilience research shows that disruptions in tightly connected systems often spread beyond the initially affected node, generating ripple effects and multi-stage recovery problems [2]. During prolonged or compound crises, these effects may escalate across operational, financial and coordination dimensions [47]. The severity of disruption, therefore, depends not only on the initiating event but on the architecture through which it moves.

Complex-network research gives this argument a broader foundation. General work on network robustness shows that the consequences of disruption depend on where failure occurs, not only on how many nodes or links are affected [8]. Motter and Lai [31] show that attacks on highly loaded nodes can trigger cascading failures through load redistribution. In interdependent networks, the problem is more severe because failure in one layer can degrade the functionality of dependent nodes in another layer [11]. Cascading-failure research further shows that such processes can become non-linear under specific dependency and load conditions [12]. Fu et al. [42] note that vulnerability analysis must also consider strategies to limit cascade transmission. For logistics, the point is straightforward: propagation depends on how the production, transport, data, energy, cloud, launch, and orbital layers are connected.

SAC is introduced as a conceptual indicator linking infrastructure configuration to disruption dynamics. It captures the extent to which an initial perturbation is magnified as it moves across layers of an interdependent logistics infrastructure. SAC is shaped by three structural properties: centrality concentration, cross-layer coupling intensity and reconfiguration capacity. It is not a calibrated predictive equation, but an assessment logic for distinguishing contained disruption from system-wide recovery demand.

SAC increases when dominant nodes and tight coupling allow disruption to cross layers. It decreases when substitute pathways, modular buffers and reconfiguration options absorb or reroute the shock. In practical terms, SAC asks whether a disturbance remains a local operational issue or becomes a broader disruption requiring recovery across the infrastructure stack. These components have already been defined methodologically; here, they are read dynamically. Centrality indicates where the shock enters, coupling determines whether it crosses layers, and reconfiguration capacity determines whether amplification can be interrupted.

When centrality and coupling are high, even modest shocks can produce disproportionate effects. A disruption at a dominant fabrication node may constrain compute availability, delay cloud expansion and affect downstream digital services. A launch bottleneck may delay the replacement of orbital assets and reduce the resilience of space-enabled data or communications functions. SAC therefore shifts attention from the probability of node failure to the amplification potential embedded in the architecture.

This is why added capacity does not automatically reduce amplification risk. A new layer improves resilience only if it creates substitutability, modularity or recovery capacity. Orbital computing illustrates the opposite possibility: a space-based layer may appear to diversify computation, yet deepen dependence on the same semiconductor bottlenecks, cloud orchestration systems, energy-intensive ground segments and launch infrastructure. In that case, the new layer adds dependency pathways rather than usable redundancy.

SAC is useful because aggregate capacity can mislead. Two systems may have similar throughput, visibility or compute capacity, but very different disruption consequences

if one concentrates critical functions in tightly coupled nodes while the other allows substitution and decoupling. Redundancy lowers SAC only when it is topologically usable, operationally accessible and independent of the same bottlenecks as the primary system.

SAC is closely related to TPV, but the two constructs are not identical. TPV describes the structural proximity of a logistics infrastructure configuration to a fragility threshold. SAC describes the expected amplification of a disturbance upon entering the system. TPV is a vulnerability condition; SAC is an amplification logic. High TPV does not always imply a very high SAC if the shock is present across cross-layer interfaces. Conversely, a moderate-TPV configuration may still exhibit high SAC if a targeted disruption affects a node that connects otherwise separable layers.

SAC can be operationalized in future research through centrality measures, interdependency matrices and indicators of substitute pathways, recovery time, spare capacity and governance constraints. Such work would require multiplex network mapping and empirical data beyond the scope of this article. The present contribution specifies the assessment logic.

The following section applies this logic through a stylized resilience assessment of alternative infrastructure configurations.

5.2. Stylized Diagnostic Assessment

To illustrate how SAC can be used as an assessment logic, this section compares two stylized infrastructure configurations. The aim is not to simulate failure, but to show how different topologies can produce different resilience outcomes with the same functional layers. The assessment focuses on four layers that are central to orbital computing and related high-technology logistics infrastructures: semiconductor fabrication, hyperscale cloud orchestration, energy infrastructure and an orbital or space-based computing layer.

The first configuration is centralized and tightly coupled. Frontier semiconductor capacity is concentrated in a small number of advanced fabrication nodes; hyperscale cloud orchestration is controlled by a few dominant providers; energy supply depends on critical regional hubs; and the orbital layer relies on limited launch and ground-segment capacity. This configuration can deliver high performance under normal conditions, but its weaknesses become apparent under disruption. A shock to a dominant fabrication node can constrain hardware availability, reduce cloud expansion capacity and delay orbital deployment or maintenance. The disruption is then amplified across the stack rather than contained locally.

The second configuration is distributed and modular. Semiconductor capacity is less concentrated, cloud orchestration is regionally modularized, energy supply includes geographically dispersed sources, and orbital compute functions are supported by multiple launch, ground-segment and control pathways. This architecture may sacrifice some economies of scale, but it increases reconfiguration capacity. If one node or layer is disrupted, demand can be rerouted, substitute capacity activated and affected layers partially decoupled. The same shock is more likely to cause local degradation than to trigger cascading disruption.

Figure 3 qualitatively compares the two configurations, illustrating relative differences in TPV, SAC, and likely resilience outcomes.

The table distinguishes TPV from SAC by treating TPV as a pre-shock property of the configuration, while SAC depends on where the shock enters and whether cross-layer transmission is contained or amplified. Both configurations may include technically advanced fabs, cloud regions, energy systems and orbital assets. The difference lies in the topology of interdependence. In the centralized configuration, dominant nodes perform load-bearing roles across layers; in the distributed modular configuration, alternative

pathways reduce the likelihood of system-wide amplification. Redundancy and modularity do not eliminate disruption; they change its propagation path. A local failure still causes degradation, but alternative pathways make amplification less likely.

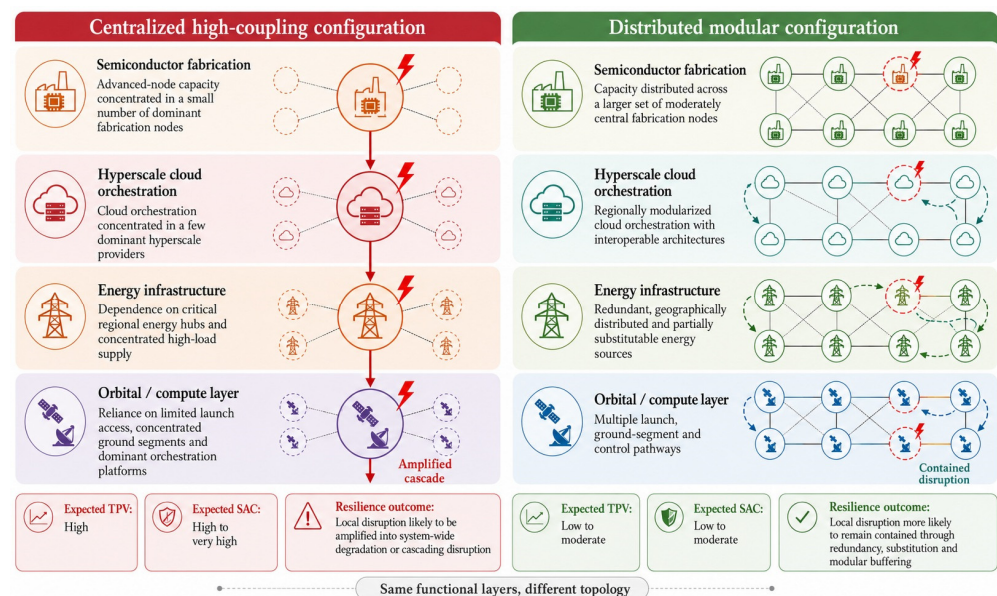


Figure 3. Stylized topology profiles: centralized high-coupling and distributed modular infrastructure configurations. Source: Author's own conceptualization.

Orbital computing is useful here as a stress test. Adding an orbital layer may appear to diversify computational geography, but it enhances resilience only if it changes the topology of dependence. If the orbital layer relies on the same concentrated semiconductor suppliers, hyperscale orchestration platforms, energy bottlenecks, and launch providers, it creates dependency pathways without providing usable redundancy. If it is designed with modular ground segments, diversified launch access, interoperable cloud architectures and redundant control pathways, it may provide buffering instead.

The assessment clarifies that high SAC is not a property of orbital computing itself. It is a property of an infrastructure configuration in which centrality concentration, tight coupling and limited reconfiguration capacity coexist.

The next section examines how redundancy, modularity, decoupling and logistics reconfiguration can reduce TPV and SAC in interdependent high-technology logistics infrastructures.

6. Resilience-Oriented Reconfiguration and Alternative Infrastructure Configurations

6.1. Redundancy, Modularity and Decoupling

Resilience is often described as a system's ability to withstand disruption, but this is too broad for the problem addressed here. Supply chain resilience research distinguishes between absorptive, adaptive and transformative capacities [1]. Absorptive resilience maintains functionality through buffers or temporary adjustments. Adaptive resilience reroutes flows, reallocates capacity or adjusts sourcing. Transformative resilience changes the underlying architecture. For TPV and SAC, this distinction matters because mitigation can either operate within an existing topology or redesign the topology to reduce amplification.

Most high-technology logistics infrastructures still rely mainly on absorptive and adaptive responses. Ripple-effect modelling and recovery frameworks typically focus on restoring functionality within an existing network structure [2]. That is useful, but

insufficient when the structure itself creates amplification risk. If dominant nodes span several layers and reconfiguration options are limited, faster recovery may still leave the same amplification pathways intact. The logistics question is therefore whether the architecture allows disruption to remain contained.

Three design principles are central here: redundancy, modularity and decoupling. Redundancy lowers SAC only when alternative capacity is independent of the same bottleneck nodes as the primary system. Modularity limits propagation by separating infrastructure functions into partly independent units. Decoupling reduces the intensity of cross-layer dependencies, so that disruptions in one layer do not immediately degrade another. This logic is consistent with interdependent infrastructure research: Rinaldi et al. [7] show why infrastructure failure must be analyzed through physical, cyber, geographic and logical dependencies, while Ouyang [6] demonstrates that vulnerability and recovery depend on dependency structures rather than isolated component reliability.

The key point is that mitigation is not the same as adding more capacity. Additional warehouses, cloud capacity, launch options or semiconductor capacity improve resilience only when they create usable alternatives. If they reinforce the same dominant nodes, they may increase SAC. Effective mitigation, therefore, requires network rewiring: redistributing centrality, weakening unnecessary coupling, adding modular buffers and improving reconfiguration capacity.

Orbital computing illustrates this design problem. It may increase SAC if it reinforces dependence on advanced-node fabrication facilities, hyperscale orchestration platforms, concentrated energy hubs and limited launch capacity. It may reduce TPV and SAC only if it is connected through diversified launch access, modular ground segments, regional fabrication ecosystems and interoperable control architectures. The same orbital layer can therefore serve either as an additional dependency or as a topological buffer.

This creates the central design tension. The most efficient architecture under normal operating conditions may not be the most resilient architecture under targeted disruption. Reconfiguration capacity is therefore not only a technical property; it is shaped by investment geography, governance rights, alliance coordination and industrial policy.

Mitigation should therefore be read as a topological design problem. Absorptive resilience protects the existing topology, adaptive resilience reroutes flows within it, and transformative reconfiguration changes the topology that enables amplification. For interdependent logistics infrastructures, the strongest resilience gains come from the third level.

6.2. Policy-Driven Reconfiguration and Controlled Fragmentation

The centrality paradox is also a policy problem. High-centrality infrastructures become strategic assets, and strategic assets attract state intervention. Semiconductor supply chains, hyperscale cloud infrastructures, and critical digital components are now shaped not only by market efficiency but also by geopolitical rivalry, security concerns, and technological industrial policy. For this paper, the relevant issue is how policy changes centrality concentration, cross-layer coupling and reconfiguration capacity.

The CHIPS and Science Act can be read not only as industrial policy but also as an attempt to redesign a vulnerable infrastructure topology [13]. Subsidies, guardrails, export controls, and strategic investment aim to reduce dependence on extreme fabrication clustering and create alternative production capacity. The resilience effect is not automatic. Policy reduces TPV and SAC only if it produces genuine dispersion, usable substitutes and recovery options. If new capacity creates another concentrated cluster, the bottleneck is relocated rather than removed.

Alliance-based coordination works through the same logic. Regional and multilateral semiconductor initiatives seek to reduce dependence on single-node chokepoints while

avoiding uncontrolled fragmentation [15,48]. Fragmentation can reduce SAC by creating modular redundancy and preventing disruption in one cluster from spreading across the whole system. It can also increase the difficulty of recovery when it produces incompatible regional blocs with limited substitutability. The system then becomes less globally centralized but not necessarily more resilient.

This is the policy version of the centrality paradox: decentralization may reduce cascade exposure, but it can also reduce pooling efficiency, slow innovation diffusion, and create interface frictions. Fragmentation improves logistics resilience only when it increases usable alternatives without creating new barriers to rerouting, substitution or repair.

Orbital computing follows the same logic. If it remains dependent on concentrated semiconductor supply, a few launch providers and hyperscale cloud orchestration, it adds another layer to the same centralized stack. If embedded in diversified launch ecosystems, modular ground segments and interoperable control architectures, it may contribute to rebalancing.

Policy-driven reconfiguration should therefore be evaluated topologically. The question is not whether intervention creates more capacity or more national control, but whether it redistributes centrality, weakens unnecessary coupling and increases reconfiguration capacity. Only then does policy-driven redesign reduce TPV and SAC rather than shift fragility into new locations.

The next section compares alternative infrastructure configurations and their implications for logistics resilience.

6.3. Comparative Infrastructure Configurations

The preceding sections developed TPV and SAC as diagnostic concepts for assessing how infrastructure topology shapes shock amplification. This section applies that logic to three stylized infrastructure configurations: hyper-centralized expansion, distributed modular rebalancing and fragmented bloc infrastructure. These are design archetypes, not predictions. They show how similar expansions in compute, semiconductor, cloud, energy or orbital capacity can produce different resilience outcomes depending on centrality, coupling and reconfiguration capacity.

In a hyper-centralized expansion, AI escalation and infrastructure scaling reinforce existing dominant nodes. Leading-edge semiconductor fabrication remains concentrated, hyperscale cloud orchestration is controlled by a small number of providers, energy demand concentrates around critical hubs, and orbital capacity depends on limited launch and ground-segment pathways. This configuration may deliver high throughput under normal conditions, but it raises TPV because critical functions become harder to bypass. SAC becomes high when disruption affects a load-bearing node and moves across dependent layers.

In a distributed modular rebalancing, capacity is intentionally dispersed across regions, interoperable cloud architectures, diversified energy sources and multiple launch or control pathways. Cross-layer coupling does not disappear, but it becomes easier to contain due to alternative pathways and modular buffers. This configuration may sacrifice some scale efficiency, but it lowers amplification potential by embedding reconfiguration capacity into the architecture.

A fragmented bloc infrastructure produces a more ambiguous resilience profile. Geopolitical segmentation, export controls and techno-national industrial strategies may reduce global dependence on a single dominant node or region [14]. However, each bloc may still develop its own internally concentrated fabrication sites, cloud platforms, energy hubs and launch providers. Fragmentation may therefore reduce global cascade exposure while preserving or increasing bloc-level fragility. Its resilience value depends on whether

regional separation creates modular redundancy or merely replaces one global bottleneck with several less interoperable regional bottlenecks.

Table 4 summarizes the paper's mechanism by linking each infrastructure configuration to its topological profile, expected TPV/SAC and logistics resilience implication.

Table 4. Logistics resilience implications of alternative infrastructure configurations.

Configuration	Topological Profile	Expected TPV/SAC	Logistics Resilience Implication
Hyper-centralized expansion	Dominant-node reinforcement; very high centrality concentration and cross-layer coupling; low reconfiguration capacity	TPV: very high SAC: high to very high	High throughput under normal conditions, but elevated risk of cross-layer cascading failure under targeted disruption
Distributed modular rebalancing	Dispersed capacity; moderate coupling; high reconfiguration capacity through substitutability, interoperability and rerouting	TPV: low to moderate SAC: low to moderate	Local disruption is more likely to remain contained through redundancy, substitution and modular buffering
Fragmented bloc infrastructure	Lower global centrality but potentially high within-bloc concentration and coupling; limited cross-bloc reconfiguration	TPV: uneven: lower globally, potentially high within blocs SAC: bounded but uneven	Lower probability of global cascades, but higher risk of bloc-level rigidity, duplication and interface friction

Note: Qualitative levels indicate relative differences between stylized configurations, not calibrated thresholds. TPV refers to the pre-shock structural vulnerability of the configuration, whereas SAC refers to the conditional amplification potential once disruption enters the system. Source: Author's own conceptualization.

The comparison shows that infrastructure scaling has no fixed effect on resilience. It can increase fragility by reinforcing dominant nodes, reduce fragility by creating usable alternatives, or shift fragility into regional blocs when fragmentation limits interoperability. Additional fabs, cloud regions, energy hubs or launch pathways reduce TPV and SAC only when they change the topology of dependence.

The configurations also suggest indicators for resilience monitoring. Rising semiconductor concentration, hyperscale cloud dependence, energy-node dependence, launch-provider concentration and cross-layer dependency density may signal increasing TPV. Greater fabrication dispersion, cloud interoperability, energy redundancy, launch diversity and usable substitution pathways may indicate topological rebalancing.

The following discussion clarifies how this perspective on topological fragility contributes to research on logistics and supply chain resilience.

7. Discussion

This paper contributes to logistics and supply chain resilience research by developing a topology-based framework for analyzing shock amplification in interdependent logistics infrastructures. Its central argument is that system-level fragility arises from the interaction among centrality concentration, cross-layer coupling, and weak reconfiguration capacity. TPV captures pre-shock structural exposure, while SAC captures conditional amplification once disruption enters the system. The framework, therefore, shifts attention from isolated assets to the architecture through which disruption moves.

7.1. Contribution to Logistics and Supply Chain Resilience Research

The paper makes three contributions. First, it conceptualizes centrality concentration as a logistics resilience bottleneck. Supply chain resilience research has long emphasized

flexibility, redundancy, visibility and recovery capacity. This paper adds that such capabilities can be undermined when functional dominance is concentrated in a small number of nodes across several infrastructure layers. A logistics infrastructure may look robust in normal operation while remaining close to a fragility threshold under targeted disruption.

Second, the paper clarifies how external disturbances act through infrastructure topology. Geopolitical rivalry, climate stress, techno-national policy and AI acceleration matter because they alter load, dependence and substitutability within the infrastructure itself. A disturbance becomes systemic when it affects a high-centrality node that connects dependent layers and cannot be quickly bypassed.

Third, the paper shows that infrastructural escalation may increase resilience or fragility depending on how new layers are connected. AI industrialization, hyperscale cloud expansion, semiconductor clustering and orbital computing may expand capacity, but they can also add dependency pathways. New layers improve resilience only when they create usable alternatives: substitutable capacity, modular interfaces, dispersed control and feasible rerouting.

Orbital computing serves as a stress case rather than as the main empirical object. Its value lies in making the logic of extreme infrastructure layering visible: additional layers may buffer disruption or amplify it, depending on their topology.

7.2. Design and Governance Implications

If logistics resilience depends on topology, then resilience governance cannot be reduced to capacity expansion. More fabs, cloud regions, launch options, or energy nodes do not automatically lower systemic risk. They do so only when they redistribute centrality, weaken unnecessary coupling and improve reconfiguration capacity.

Three design implications follow. First, centrality dispersion should become a resilience objective. Industrial policy, public procurement, alliance frameworks, and infrastructure investment can be assessed not only by their output effects, but also by whether they reduce dependence on dominant nodes across the semiconductor, cloud, energy, and launch layers. The objective is not decentralization for its own sake, but the reduction in single-node dominance where that dominance creates disproportionate cascade potential.

Second, modularity and decoupling should be treated as design principles for infrastructure. Interoperable standards, distributed ground segments, regional redundancy, and modular control architectures can help keep local degradation local. This is particularly important where replacement cycles, launch constraints, or ground-segment dependence slow recovery.

Third, centrality monitoring should complement conventional logistics resilience metrics. Lead time, capacity utilization, delivery reliability and inventory availability remain useful, but they do not reveal hidden amplification exposure. Relevant additional indicators include the dispersion of advanced fabrication capacity, hyperscale cloud concentration, energy-node dependence, launch-provider concentration, ground-segment redundancy and cross-layer dependency density. These indicators would add an infrastructure-architecture layer to existing supply chain risk tools.

These principles do not imply that centralized infrastructures are always undesirable. Centralization may improve efficiency, standardization and coordination. The problem arises when concentration creates load-bearing nodes that cannot be bypassed during disruption. The governance challenge is therefore to balance scale economies with substitutability, interoperability and recovery options.

7.3. Future Assessment and Limitations

The framework also has methodological implications. Conventional supply chain resilience assessment often starts with suppliers, buffers, contingency plans, recovery procedures and flow restoration. Topological fragility analysis starts one step earlier, with the architecture of interdependence. It asks which nodes are structurally dominant, which layers depend on them and whether disruption pathways are buffered or amplified.

A practical assessment would map infrastructure layers, identify critical nodes, estimate centrality concentration, trace cross-layer dependencies and assess reconfiguration capacity. This is especially relevant where physical flows, digital orchestration, energy availability and specialized production capacity are tightly interdependent.

The main limitation is that the framework remains conceptual and stylized. It does not provide calibrated TPV thresholds or a numerical SAC model. Future research should operationalize the framework through multiplex network modelling, simulation, dependency matrices and empirical case studies of semiconductor–cloud–energy–orbital interdependence. Such work could test whether systems with similar operational capacity but different centrality distributions exhibit different cascade behaviour under targeted shocks. Further studies should also examine how centrality monitoring and cross-layer dependency mapping can be integrated into logistics resilience planning.

The value of the present framework is therefore diagnostic. It does not predict disruption probabilities. It identifies the structural conditions under which disruption is more likely to be amplified. For research on logistics and supply chain resilience, this is a necessary step: next-generation logistics infrastructure will be judged not only by the capacity it creates but also by whether that capacity remains usable when dominant nodes are disrupted.

8. Conclusions: Topology and Resilience in Interdependent Logistics Infrastructure

This paper has argued that the resilience of next-generation logistics infrastructure depends not only on physical feasibility, capacity expansion and digital coordination, but also on structural configuration. High-technology infrastructures increasingly combine semiconductor fabrication, hyperscale cloud orchestration, energy systems, launch logistics and orbital or space-enabled assets. These layers can expand capability, but they can also create new disruption pathways when critical functions are concentrated and tightly coupled.

The paper conceptualized this problem through TPV and SAC. TPV captures the pre-shock proximity of an infrastructure configuration to a structural fragility threshold, while SAC captures conditional amplification once disruption enters the system. Together, the constructs explain why systems with similar operational capacity may produce different resilience outcomes when their topologies differ.

Orbital computing was used as an extreme illustrative context rather than as a prediction about the near-term future of space-based data infrastructure. Its value lies in making the logic of interdependence visible. An orbital layer improves resilience only when it changes the topology of dependence by adding usable alternatives, modular interfaces and independent recovery pathways.

The framework remains conceptual and should be operationalized through multiplex network modelling, infrastructure dependency matrices, simulations of targeted disruptions and comparative case studies of semiconductor–cloud–energy–launch interdependence. The main message is simple but consequential: the challenge for orbital computing and other high-technology logistics infrastructures is not only technical feasibility, but the management of topological fragility.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Acknowledgments: During the preparation of this work, the author used ChatGPT 5.5 Thinking (OpenAI) and Consensus to support language editing and identify relevant academic literature. After using these tools, the author carefully reviewed and edited the manuscript and takes full responsibility for the content of the published article.

Conflicts of Interest: The author declares no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial intelligence
SAC	Shock Amplification Coefficient
TPV	Topological Phase Vulnerability

References

1. Tukamuhabwa, B.R.; Stevenson, M.; Busby, J.; Zorzini, M. Supply chain resilience: Definition, review and theoretical foundations for further study. *Int. J. Prod. Res.* **2015**, *53*, 5592–5623. [\[CrossRef\]](#)
2. Katsaliaki, K.; Galetsi, P.; Kumar, S. Supply chain disruptions and resilience: A major review and future research agenda. *Ann. Oper. Res.* **2022**, *319*, 965–1002. [\[CrossRef\]](#) [\[PubMed\]](#)
3. Guo, Z.; Zhang, Y.; Zhao, X.; Song, X. CPS-Based Self-Adaptive Collaborative Control for Smart Production-Logistics Systems. *IEEE Trans. Cybern.* **2021**, *51*, 188–198. [\[CrossRef\]](#) [\[PubMed\]](#)
4. Conrad, S.H.; LeClaire, R.J.; O'Reilly, G.P.; Uzunalioglu, H. Critical national infrastructure reliability modeling and analysis. *Bell Labs Tech. J.* **2006**, *11*, 57–71. [\[CrossRef\]](#)
5. Johansson, J.; Hassel, H. An approach for modelling interdependent infrastructures in the context of vulnerability analysis. *Reliab. Eng. Syst. Saf.* **2010**, *95*, 1335–1344. [\[CrossRef\]](#)
6. Ouyang, M. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliab. Eng. Syst. Saf.* **2014**, *121*, 43–60. [\[CrossRef\]](#)
7. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Syst. Mag.* **2001**, *21*, 11–25. [\[CrossRef\]](#)
8. Artime, O.; Grassia, M.; De Domenico, M.; Gleeson, J.P.; Makse, H.A.; Mangioni, G.; Perc, M.; Radicchi, F. Robustness and resilience of complex networks. *Nat. Rev. Phys.* **2024**, *6*, 114–131. [\[CrossRef\]](#)
9. Zarghami, S.A.; Dumrak, J. Unearthing vulnerability of supply provision in logistics networks to the black swan events: Applications of entropy theory and network analysis. *Reliab. Eng. Syst. Saf.* **2021**, *215*, 107798. [\[CrossRef\]](#)
10. Engsig, M.; Tejedor, A.; Moreno, Y.; Foufoula-Georgiou, E.; Kasmi, C. DomRank Centrality reveals structural fragility of complex networks via node dominance. *Nat. Commun.* **2024**, *15*, 56. [\[CrossRef\]](#) [\[PubMed\]](#)
11. Buldyrev, S.V.; Parshani, R.; Paul, G.; Stanley, H.E.; Havlin, S. Catastrophic cascade of failures in interdependent networks. *Nature* **2010**, *464*, 1025–1028. [\[CrossRef\]](#) [\[PubMed\]](#)
12. Valdez, L.D.; Shekhtman, L.; La Rocca, C.E.; Zhang, X.; Buldyrev, S.V.; Trunfio, P.A.; Braunstein, L.A.; Havlin, S. Cascading failures in complex networks. *J. Complex Netw.* **2020**, *8*, cnaa013. [\[CrossRef\]](#)
13. Luo, Y.; Van Assche, A. The rise of techno-geopolitical uncertainty: Implications of the United States CHIPS and Science Act. *J. Int. Bus. Stud.* **2023**, *54*, 1423–1440. [\[CrossRef\]](#) [\[PubMed\]](#)
14. Liu, Q.; Xue, D.; Li, W. A Sustainable Production Segment of Global Value Chain View on Semiconductors in China: Temporal and Spatial Evolution and Investment Network. *Sustainability* **2024**, *16*, 8617. [\[CrossRef\]](#)
15. Rolf, S.; Baines, J.; Germann, J.; Starrs, S. The geographies and geopolitics of industrial policy: Designing a data-driven UK semiconductor strategy. *Eur. Urban Reg. Stud.* **2025**, *32*, 115–123. [\[CrossRef\]](#)

16. Christopher, M.; Peck, H. Building the Resilient Supply Chain. *Int. J. Logist. Manag.* **2004**, *15*, 1–14. [[CrossRef](#)]
17. Ponomarov, S.Y.; Holcomb, M.C. Understanding the concept of supply chain resilience. *Int. J. Logist. Manag.* **2009**, *20*, 124–143. [[CrossRef](#)]
18. Pettit, T.J.; Fiksel, J.; Croxton, K.L. Ensuring supply chain resilience: Development of a conceptual framework. *J. Bus. Logist.* **2010**, *31*, 1–21. [[CrossRef](#)]
19. Pettit, T.J.; Croxton, K.L.; Fiksel, J. The Evolution of Resilience in Supply Chain Management: A Retrospective on Ensuring Supply Chain Resilience. *J. Bus. Logist.* **2019**, *40*, 56–65. [[CrossRef](#)]
20. Wieland, A.; Durach, C. Two perspectives on supply chain resilience. *J. Bus. Logist.* **2021**, *42*, 315–322. [[CrossRef](#)]
21. Hosseini, S.; Ivanov, D.; Dolgui, A. Review of quantitative methods for supply chain resilience analysis. *Transp. Res. Part E Logist. Transp. Rev.* **2019**, *125*, 285–307. [[CrossRef](#)]
22. Hosseini, S.; Ivanov, D.; Blackhurst, J. Conceptualization and Measurement of Supply Chain Resilience in an Open-System Context. *IEEE Trans. Eng. Manag.* **2022**, *69*, 3111–3126. [[CrossRef](#)]
23. Ivanov, D.; Sokolov, B.; Dolgui, A. The Ripple effect in supply chains: Trade-off ‘efficiency-flexibility-resilience’ in disruption management. *Int. J. Prod. Res.* **2014**, *52*, 2154–2172. [[CrossRef](#)]
24. Dolgui, A.; Ivanov, D.; Sokolov, B. Ripple effect in the supply chain: An analysis and recent literature. *Int. J. Prod. Res.* **2018**, *56*, 414–430. [[CrossRef](#)]
25. Maharjan, R.; Kato, H. Resilient supply chain network design: A systematic literature review. *Transp. Rev.* **2022**, *42*, 739–761. [[CrossRef](#)]
26. Ivanov, D. Viable supply chain model: Integrating agility, resilience and sustainability perspectives—Lessons from and thinking beyond the COVID-19 pandemic. *Ann. Oper. Res.* **2022**, *319*, 1411–1431. [[CrossRef](#)] [[PubMed](#)]
27. Ivanov, D.; Dolgui, A.; Blackhurst, J.V.; Choi, T.-M. Toward supply chain viability theory: From lessons learned through COVID-19 pandemic to viable ecosystems. *Int. J. Prod. Res.* **2023**, *61*, 2402–2415. [[CrossRef](#)]
28. Yang, Y.; Pan, S.; Ballot, E. Mitigating supply chain disruptions through interconnected logistics services in the Physical Internet. *Int. J. Prod. Res.* **2017**, *55*, 3970–3983. [[CrossRef](#)]
29. Yu, J.; Zhou, C.; Leng, G. Is It Always Advantageous to Establish Self-Built Logistics for Online Platforms in a Competitive Retailing Setting? *IEEE Trans. Eng. Manag.* **2024**, *71*, 1726–1743. [[CrossRef](#)]
30. Albert, R.; Jeong, H.; Barabási, A.-L. Error and attack tolerance of complex networks. *Nature* **2000**, *406*, 378–382. [[CrossRef](#)] [[PubMed](#)]
31. Motter, A.E.; Lai, Y.-C. Cascade-based attacks on complex networks. *Phys. Rev. E* **2002**, *66*, 065102. [[CrossRef](#)] [[PubMed](#)]
32. Ho, K. Space Logistics Modeling and Optimization: Review of the State of the Art. *J. Spacecr. Rocket.* **2024**, *61*, 1417–1427. [[CrossRef](#)]
33. Whetten, D.A. What Constitutes a Theoretical Contribution? *Acad. Manag. Rev.* **1989**, *14*, 490–495. [[CrossRef](#)]
34. Jaakkola, E. Designing conceptual articles: Four approaches. *AMS Rev.* **2020**, *10*, 18–26. [[CrossRef](#)]
35. Zadeh, L.A. Fuzzy sets. *Inf. Control* **1965**, *8*, 338–353. [[CrossRef](#)]
36. Ragin, C.C. *Redesigning Social Inquiry: Fuzzy Sets and Beyond*; University of Chicago Press: Chicago, IL, USA, 2009.
37. George, A.L.; Bennett, A. *Case Studies and Theory Development in the Social Sciences*; MIT Press: Cambridge, MA, USA, 2005.
38. Kazim, M.; Pirim, H.; Shi, S.; Wu, D. Multilayer analysis of energy networks. *Sustain. Energy Grids Netw.* **2024**, *39*, 101407. [[CrossRef](#)]
39. Kazim, M.; Pirim, H.; Le, C.; Le, T.; Yadav, O.P. Link Prediction and Navigability of Multiplex Energy Networks. *arXiv* **2025**, arXiv:2503.14641. [[CrossRef](#)]
40. Sahu, A.; Davis, K.; Huang, H.; Ummnakwe, A.; Zonouz, S.; Goulart, A. Design of Next-Generation Cyber-Physical Energy Management Systems: Monitoring to Mitigation. *IEEE Open Access J. Power Energy* **2023**, *10*, 151–163. [[CrossRef](#)]
41. Zografopoulos, I.; Ospina, J.; Liu, X.; Konstantinou, C. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. *IEEE Access* **2021**, *9*, 29775–29818. [[CrossRef](#)]
42. Fu, G.; Dawson, R.; Khoury, M.; Bullock, S. Interdependent networks: Vulnerability analysis and strategies to limit cascading failure. *Eur. Phys. J. B* **2014**, *87*, 148. [[CrossRef](#)]
43. van der Vlist, F.; Helmond, A.; Ferrari, F. Big AI: Cloud infrastructure dependence and the industrialisation of artificial intelligence. *Big Data Soc.* **2024**, *11*, 20539517241232630. [[CrossRef](#)]
44. Imoize, A.L.; Adediji, O.; Tandiya, N.; Shetty, S. 6G Enabled Smart Infrastructure for Sustainable Society: Opportunities, Challenges, and Research Roadmap. *Sensors* **2021**, *21*, 1709. [[CrossRef](#)] [[PubMed](#)]
45. Korkali, M.; Veneman, J.G.; Tivnan, B.F.; Bagrow, J.P.; Hines, P.D.H. Reducing Cascading Failure Risk by Increasing Infrastructure Network Interdependence. *Sci. Rep.* **2017**, *7*, 44499. [[CrossRef](#)] [[PubMed](#)]
46. Lee, C.; Tien, I. Impacts of varying network parameters on the vulnerability and resilience of interdependent critical infrastructure systems. *Sustain. Resilient Infrastruct.* **2022**, *7*, 984–1007. [[CrossRef](#)]

47. Ozdemir, D.; Sharma, M.; Dhir, A.; Daim, T. Supply chain resilience during the COVID-19 pandemic. *Technol. Soc.* **2022**, *68*, 101847. [[CrossRef](#)] [[PubMed](#)]
48. Kobayashi, T. Supply Chains, Digital Governance, and Strategic Coordination in the Indo-Pacific: A Case Study of Japan's Semiconductor Policy. *J. World Invest. Trade* **2025**, *26*, 648–679. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.