Global Supply Chain Disruptions and Strategic Risk Management in International Business Networks

Kittisak Wongchai[1*], Siriporn Saengsri[2]

[1*]*Siam Centre for Professional Excellence, Bangkok, Thailand.*

[2]*Siam Centre for Professional Excellence, Bangkok, Thailand.*

Received: 10 January 2024; Revised: 26 January 2024; Accepted: 13 February 2024; Published: 29 March 2024

Abstract

Purpose: This study seeks to analyze the reasons why disruptions spread asymmetrically through international supply chains and ways to go from reactive continuity strategies to proactive risk management. Methodology: Theory-based conceptual synthesis incorporates the ideas of supply chain resilience, resource dependence, dynamic capabilities, and interorganizational governance. Findings: The model differentiates between exposure and vulnerability; highlights visibility and coordination of decision-making powers as strategies of disruption containment; and suggests a phased portfolio of prevention, absorption, adaptation, and renewal strategies. Instead of seeing redundancy and efficiency as opposing goals that apply to all situations, the model focuses on contingencies of buffer strategies, diversified suppliers, flexibility, digital intelligence, and cooperative contracting. Originality: This study creates a risk architecture at the network level connecting disruptions' features, channels of propagation, responses and performances. This study proposes an assessment matrix, three process models that can be edited, and propositions for future studies in multiple countries. There is no primary data set; all causal links are conceptual.

Keywords: Global Supply Chains; Disruption Propagation; Strategic Risk Management; Supply Network Resilience; International Business; Dynamic Capabilities; Geopolitical Uncertainty.

I. INTRODUCTION

1.1. International Business Networks Under Compound Uncertainty

International business networks manage procurement, production, logistics, finance, and access to markets beyond corporate and national borders. The geographical scope allows for specialization and economies of scale; however, it also makes the networks reliant upon transportation networks, concentrated sources of supply, regulation, and information systems. As a result, disruption cannot be seen as only a temporary interruption at the local level. An incident in one place can influence time, cost, quality, or even legal aspects of other transactions in the network (Emrouznejad et al., 2023; Habibi et al., 2023; Gaudenzi et al., 2023). Recent studies into supply chain risk management have explored various approaches to risk identification, risk assessment, risk mitigation, and the new technologies in use in this field (Emrouznejad et al., 2023). Variability of operations needs to be differentiated from infrequent yet high-impact events that go beyond standard planning assumptions. A firm can continue operating even when there is no ability to export its products due to a restriction, or it can keep

using a transportation network even when it faces problems with higher insurance prices and greater variability of shipments.

1.2. Strategic Management Problem and Research Gap

Traditionally, approaches of assessing risks in supply chains have used measures like hazard probability, hazard impact, and hazard-mitigation strategies by function. While these frameworks have provided a good platform for risk identification and accountability, they do not provide ways of incorporating the network interdependencies that are required to determine if an affected firm is vulnerable in terms of operations. Number of suppliers is one factor that might exaggerate diversification where there are several suppliers who have common upstream materials, geographical locations, energy systems, and transportation routes. Literature has been developing in a manner that integrates resilience capabilities and appropriate responses rather than focusing on hazard mitigation strategies alone. Literature has been synthesizing concepts in resilience of supply chains as well as identifying future areas of research in the area of supply chain resilience.

Another limitation involves the treatment of efficiency and resilience as competing goals and the reliance on recovery speed as an indicator of resilience. This may ignore the necessity of balancing prevention, absorption, adaptation, and renewal of networks. The integration of structural dependencies analysis, selection of response portfolio, and cross-organizational decision making is thus an important concept. This study tackles the issue by providing a strategic risk management framework that recognizes the distinction between exposure and vulnerability, measures resilience as a collection of responses, and links operational restoration to network sustainability. Instead of asserting causality, this model produces five theoretical hypotheses that can be tested empirically in the future.

1.3. Research Objectives and Contribution

This research aims at achieving four main objectives which include: categorizing disruptive pathways related to global networks, describing how structural interdependencies contribute to shock amplification or attenuation, devising a strategic response approach that considers efficiency-resilience compromises, and identifying important governance and measurements issues in management implementations. The contribution made by this research includes a theoretical model which is multilevel, relating events' attributes to network vulnerability, organization capacities, coordination, and performance outcomes.

In other words, the study takes off from a conceptual framework based on theories to an architectural design of risks, interpretive results, managerial implications and future research agenda. The hypotheses are proposed for testing and not to be taken as causal effects.

II. THEORETICAL FOUNDATIONS AND CRITICAL LITERATURE SYNTHESIS

2.1. From Linear Chains to Interdependent Networks

A linear model of a supplier-manufacturer-customer chain is easy to use when analyzing process control issues, but it is insufficient when considering shared upstream inputs, logistical centers, financial links, and third-party digital services. A network approach focuses on the concentration of key dependencies, substitute presence, and potential impacts that disruptions

may have on related organizations. Research into supply chain resilience and adaptation to disruptions gives a theoretical background to analyze possible ways of reconfiguring supply chain networks after the disruption occurred (Al Naimi et al., 2022). Digital technologies can affect network integration and reaction to disruptions in terms of organizational response. The connection between digital technologies, integration, and firm resilience makes clear that in addition to the physical structure of a supply network, one needs to consider information and coordination processes between supply network members (Cui et al., 2023). Thus, the strategic importance of the particular supplier or logistic center should be estimated depending on its substitutability, dependencies with other network members, and effects of its disruption on the entire network.

2.2. Resilience, Robustness, and Viability

Robustness is the maintenance of performance under a disruption condition, whereas resilience is about the ability to absorb shocks, recover and adapt performance. Viability goes beyond the scope of the above two concepts and looks into the sustainability of the system in meeting its key functions in changing conditions. These concepts are related to each other, yet they should not be mixed. Buffer stock could be helpful for maintaining continuity, whereas adjustment of the product specification in order to accept substitutes could help in adaptation. Practices of supply chain risk management could have implications for the impact of a disruption on resilience and robustness of the network, illustrating the significance of differentiating between these performance measures in assessing risk management strategies (El Baz & Ruel, 2021; Wulandhari et al., 2023). Recovery period is not enough for measuring resilience, since a network could restart faster yet much more costly, with reduced service level and increased susceptibility to future disruptions.

2.3. Dynamic Capabilities and Interorganizational Coordination

Dynamic capabilities constitute a management view of organizational identification of changes, organization's response to mobilize available options, and transformations of resources in conditions of uncertainty. For supply networks, sensing is associated with the visibility of supplier environment, logistics performance, as well as changes in technology or market demands. Seizing entails re-allocating orders, utilizing alternative paths or alternative product configurations. Transformation implies investments in modularity, supplier development, and governance mechanisms which would continue to serve beyond the current crisis. Digitalization and analytics could facilitate such processes through better information and decision making. Procurement digitalization has been studied in the context of supply chain resilience, while artificial intelligence has been considered as a tool facilitating supply chain resiliency (Harju et al., 2023; Naz et al., 2022; Shishodia et al., 2023). Practices of risk management in supply chains and analytic capabilities constitute a framework for studying organizational response to disruptions (Liu & Wei, 2022). The application of Industry 4.0 technologies could be another source of proactive risk management through increased visibility of the supply chain and information processing, although this possibility depends on context (Spieske & Birkel, 2021).

But technical capability does not mean coordination in itself. The buyer may find an alternate vendor but fail to mobilize the same if the information on qualifications is not available, if the terms of contract do not allow, or if there is not enough capacity in the vendor. This aspect should be considered in the proposed framework as well.

2.4. Institutional Fragmentation and Geopolitical Exposure

Cross-border operations will encounter discrepancies in customs practices, labor laws, sanctions, data legislation, quality of infrastructure, and emergency plans. Differences of that nature are not only contextual factors but can alter the set of possible actions in response to them. An ostensibly viable supplier becomes an unsuitable one due to an inability to certify, comply with trade regulations, or settle payments in the specified timeframe. The difference between resilience and robustness in international value chains holds relevance for the discussion of international trade and policy considerations as well Miroudot, (2020). Information integrity is yet another relevant aspect of cross-organizational risks. Misinformation and disinformation can pose a threat to supply chain security, and blockchain technology has been investigated as means of addressing those issues (Petratos & Faccia, 2023). These risks clearly show that the network disruptions can occur not only due to physical limitations, but also due to inadequate information flow. The use of technology in risk analysis may help in recognizing and analyzing new risks. Machine learning techniques have been discussed in relation to supply chain risk management, where their role as well as future possibilities of research have been highlighted (Yang et al., 2023).

However, analytical instruments have to be viewed in the context of the limitations that the institutions and operation have to overcome in order to tackle the risks that have been identified. It is possible that geopolitical, regulatory, and infrastructure risks might impact more than one supplier at the same time. The manager has to distinguish between diversification by organization and diversification by other means. The pertinent issue is how these alternatives may fail collectively through credible disruption scenarios, as opposed to whether these options individually appear on any vendor list. Collectively, the literature points to an integrated approach towards strategic risk management involving consideration of factors such as network structures, resilience capacities, information systems, coordination and institutional exposures. The methodology below captures the above-mentioned issues within a conceptual framework while making no claims that the above cited literature exhausts the subject matter or that the relationships proposed have been empirically established yet.

III. RESEARCH DESIGN AND ANALYTICAL APPROACH

3.1. Conceptual Synthesis Strategy

The research on supply chain network resilience, dynamic capabilities, resource dependence, and interorganizational governance is considered foundational and contemporary for this study. The conceptual synthesis was structured along the following four dimensions: disruption nature, structural network dependencies, strategic response options, and the resilience performance outcomes. The chosen pieces of literature were reviewed in order to detect the commonalities in the conceptualization of these dimensions, different theoretical emphases, and gaps in their integration. Special focus was put on the issues of substitutability, network coupling, visibility of sub-tier members, response flexibility, and interorganizational governance. Further, the chosen

dimensions were used in order to elaborate the proposed risk architecture and five theoretical propositions. As the study does not utilize a systematic literature review methodology and empirical data set, the developed framework should be viewed as a conceptual contribution informed by theory.

3.2. Unit of Analysis and Construct Boundaries

The focal unit is the international business network managed by the lead firm, but acknowledging the fact that the suppliers and logistics providers are independent organizations. Disruption exposure is the interaction with the threat, whereas vulnerability refers to the degree to which exposure may threaten core processes. The response capability is an action taken that is viable and timely, while resilience performance refers to continuity and adaptability attained. It helps to avoid the circular statement that a resilient firm performs well because it has resilience.

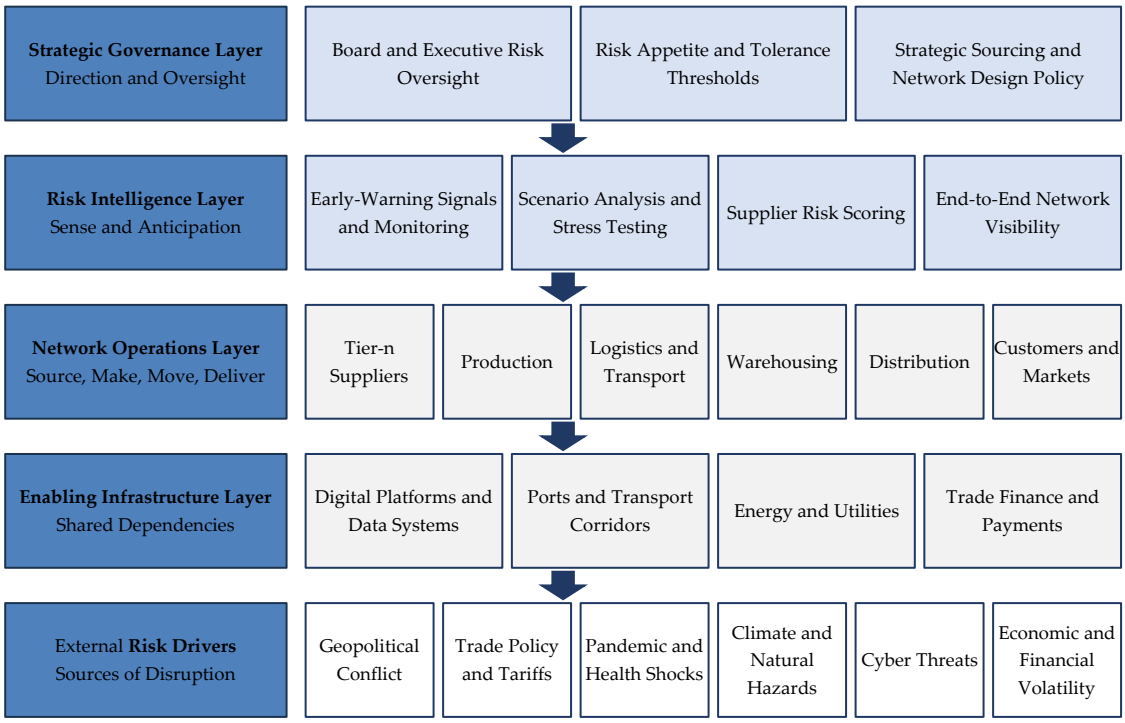

Figure 1: Multi-Layer Risk Architecture Linking Shocks, Structural Exposure, Managerial Response, and Outcomes

As seen in figure 1, even the level of severity does not determine the loss by itself. The same shock coming from outside may have different effects based on common mode dependencies, organizational limitations, and the timeliness of the response to such a shock.

3.3. Analytical Propositions and Explanatory Logic

These propositions arise from complementary theoretical explanations as opposed to being based on observations. The network dependency theory indicates that highly coupled and concentrated networks will have limited avenues for substitutions. According to the dynamic capability's theory, fast sense-making and reconfiguration minimize the persistence of disruptions. The theory of relational governance states that partners who have set escalation rules and credible information exchange processes will have minimal response delays.

1. P1 (Dependency Concentration): Greater concentration of important sub-tier dependencies leads to increased disruption vulnerability, provided that substitutability is low, lead times are long, and logistics routes are common.
2. P2 (Sensing vs. Authorization): Sub-tier visibility is effective in minimizing disruption persistence only when accompanied by pre-authorized decision-making authority and fast escalation procedures.
3. P3 (Response Portfolio): A combination of strategies that include buffers, alternate suppliers, and capacity flexibility performs better for continuity management than a redundancy strategy alone.
4. P4 (Interorganizational Governance): High interorganizational coordination quality, which involves mutual trust, agreed-upon escalation procedures, and harmonized incentives, improves the association between response capabilities and recovery speed.
5. P5 (Learning & Viability): Post-event structure learning and network re-design help in enhancing network viability, apart from operational recovery alone.

These five propositions represent theoretical relationships that should hold, not empirically proven causalities. The applicability of these relationships could depend on the level of disruption, importance of the disrupted product, regulatory requirements in an industry, bargaining power of suppliers, and availability of alternative suppliers. In future research, it will be important to consider not only these relationships but also conditions under which they can become stronger, weaker, or different.

3.4. Evidence Interpretation and Validity Safeguards

This paper distinguishes between well-understood concepts and new ideas. It makes no attempt at deriving an estimate for the size of the effect, its statistical significance, or the effectiveness of a certain approach to procurement. The following contradictory situations are taken into account: diversification might complicate the task and make it more expensive; inventory might become obsolescent; nearshoring might bring concentration of risk in another kind of danger; and real-time visibility might have cybersecurity or governance implications.

3.5. Proposed Future Empirical Design

Future research could utilize network-level transaction data, supplier mapping, records of disruptions that occurred, and manager interviews from several industries. Measures of exposure to risk would have to take into account geographical and sub-tier concentration, dependency criticality, switching costs, and corridor redundancy. Capability would need to be measured via documented alert to decision time, readiness for qualification, and procedures for escalation. The consequences would need to include service failure, recovery time, margin consequences, and network structure change after the disruption. Multilevel models or an event study approach would allow testing of the propositions, while controlling for industry type, firm size, shock intensity, and the institutional context. When surveys are conducted, it should ensure content validity via expert judgment, reliability and discrimination via appropriate measurement tests, and method specificity via multiple respondent sources or archival measures.

IV. CONCEPTUAL FINDINGS: HOW DISRUPTIONS BECOME NETWORK CRISES

4.1. The Escalation Mechanism

This synthesis highlights that there is a mechanism where the impact of a triggering factor happens once there is interaction with an operational dependence factor. A late delivery may be managed if there is safety stock and/or capacity; however, the same late delivery would stop production if there was only one certified supplier for which no other supplier is able to provide a similar product. The initial effects of the triggering event then cascade due to coordinated scheduling, contractual obligations, financial pressure, and customer service. This mechanism has a temporal aspect. Initial indications may be ambiguous and managers wait before making decisions to reduce costs. However, once a disruption takes place, the decision space narrows due to already used transport capacity, inventory, and suppliers.

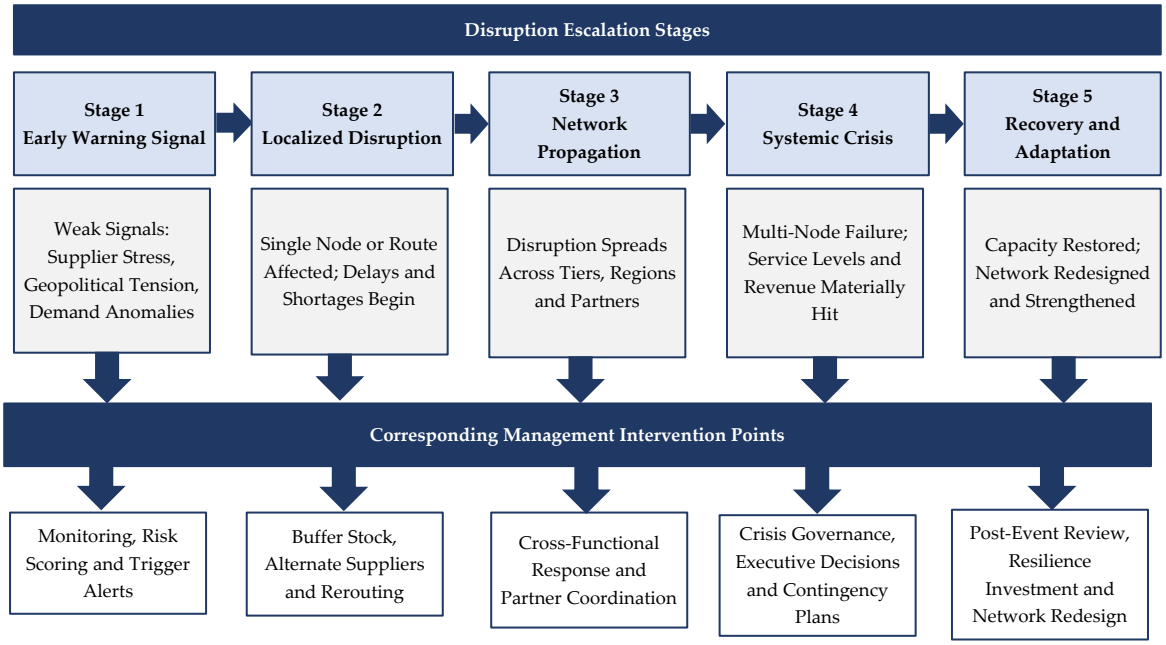

Figure 2: Disruption Escalation Stages and Corresponding Management Intervention Points

Disruptions in a supply chain can progress from being local disturbances to becoming disruptive at the level of the entire supply chain network as depicted in figure 2. This figure shows the points of intervention which can reduce the spread of these disturbances.

4.2. Structural Drivers of Vulnerability

There are five drivers that feature repeatedly in the literature: reliance on scarce inputs, clustering, high synchronization, lack of transparency at the sub-level, and low substitutability. The effects of such drivers tend to be synergistic. High concentration can be easily managed if the part is generic and stock levels are sufficient; on the other hand, moderate concentration can prove highly risky when certifications and special tools take time to change.

4.3. Risk Archetypes and Strategic Implications

Various types of shocks call for various response mixes. Short-term disruptions may call for rerouting and inventory re-allocation, while longer-term restrictions may necessitate qualifying

suppliers and renegotiating contracts, while cyber-attacks may call for separation of information dependencies and manual contingency plans. The general advice to "increase redundancy" would then be meaningless. Table 1 summarizes strategic options based on failure modes and time frames.

Table 1: Network Disruption Archetypes and Response Logic

Risk archetype	Transmission mechanism	Near-term priority	Strategic redesign
Supplier capacity loss	Shortage of critical inputs and late replenishment	Allocating Inventory; Activating Qualified Alternate	Dual certification; portable tooling
Logistics corridor disruption	Transit delays and freight capacity shortage	Divert; give priority to mission-critical orders	Multicorridor layout; routing agreements
Trade or regulatory shock	Ineligibility for market or supply sourcing	Review for compliance; substitute legally	Regionalism; regulatory information
Cyber or data outage	Visibility loss in planning and coordination	Isolated systems; manual control	Digital segmenting; recovery exercises
Climate or infrastructure event	Facility and utility disruption correlation	Prioritize safety; reallocate resources	Geographic hazard spreading

Matrix is an analytic categorization tool and not a frequency distribution chart. It explains why response efficacy relies on the compatibility of the mechanism used to disrupt an organization and its capacity. For instance, an alternative source that has not been qualified by relevant regulators will offer little protection from a sudden border closure.

4.4. Efficiency–Resilience Trade-Offs as Portfolio Choices

Efficiency versus resilience can be perceived as an either-or question regarding being lean or having excess capacity. The proper way to look at it is through scenario management and portfolio optimization. Strategic buffers can be created in case of high service criticality and high lead times of certain items. Flexible agreements can retain optional capacity without buying it continuously. Modularity of products can increase substitutability among different suppliers. The tools vary by their cost, speed, and sustainability characteristics. Portfolio management should also incorporate correlation issues. In case two suppliers offer redundancy, but they are dependent on the same power supply network, chemical input, or sea route. Proper diversification involves dependency mapping and scenario analysis. The optimal portfolio is not always the biggest portfolio; it is the right portfolio that maintains response capacity in case of disruptions to the organization (Table 2).

Table 2: Criteria for Supply Chain Resilience Portfolio Selection

Response Option	Main Benefit	Main Limitation	Decision Criterion
Strategic inventory buffers	Absorbs temporary disruptions in supply	Storage expenses and inventory deterioration	Material criticality and replenishment lead time
Qualified alternative suppliers	Decreases reliance on one particular supplier	Costs of qualifying and switching time	Availability and capability of alternative providers
Flexible production capacity	Facilitates shifting of production in disruptions	Capacity booking and operational costs	Demand fluctuations and capacity activation time
Alternative logistics routes	Decreases dependency on one route for transport	Higher transportation costs and route limitations	Demand fluctuations and capacity activation time
Digital risk visibility	Fosters early disruption identification and intelligent decision making	Cybersecurity and data management threats	Capability to respond and data quality

V. STRATEGIC RISK MANAGEMENT FRAMEWORK

5.1. Governance Architecture for Cross-Border Decisions

Strategic risk management demands an appropriate separation of network-level risk ownership from operational authority on the ground. Central management has the responsibility to set risk appetite, thresholds for service, and escalation rights. Regional staff needs to understand local regulatory and infrastructure environment, whereas suppliers and logistics service providers have to deliver capacity and exception data according to established protocols. Otherwise, increased visibility may enhance awareness but not speed up action. Governance can be designed so that owners of decisions related to critical dependencies are appointed, and appropriate response options are pre-approved up to specified costs and regulations. The procedures for escalation must clearly define who will have the right to approve alternate sourcing, special air freight, repositioning of inventories, and even substituting products.

Figure 3 displays a risk operation framework that relates risk intelligence, decision governance, implementation coordination, and organizational learning. It shows how continuous information collection and decision-making processes enable an organization to respond to any disturbances, and through post-disruption evaluation, a better strategy is developed for future risk management.

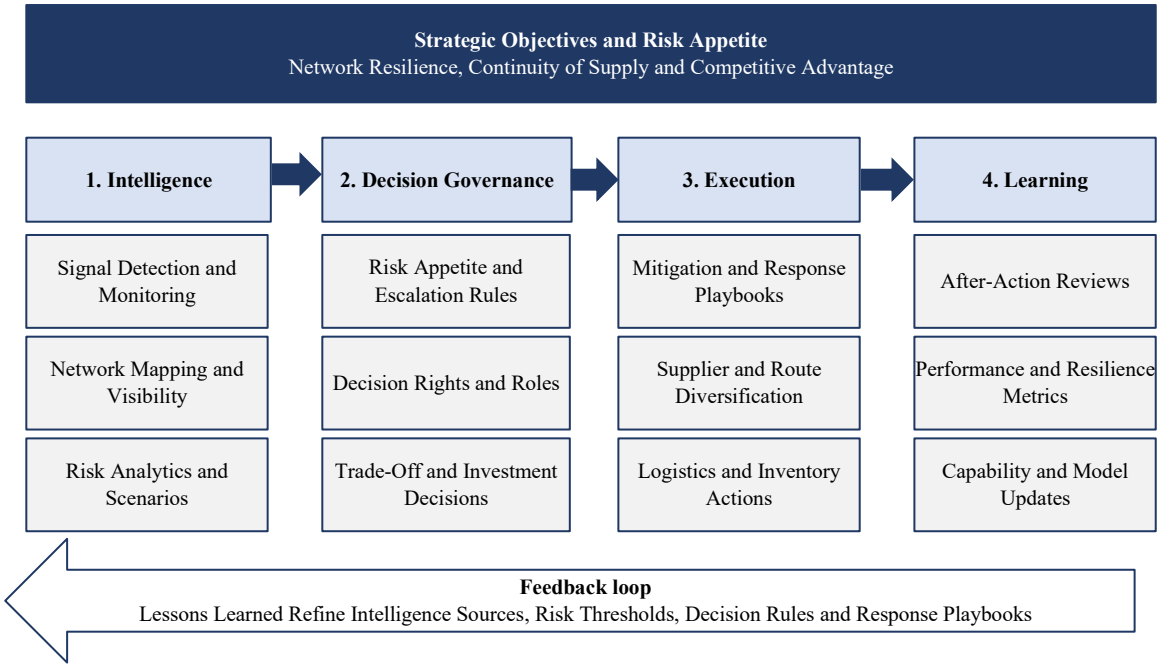

Figure 3: Strategic Risk Operating Model Integrating Intelligence, Decision Governance, Execution, and Learning

5.2. Risk Prioritization and Response Selection

The process of prioritization ought to begin with critical business outcomes, such as delivery of goods to customers, compliance requirements, or required level of production capacity. Managers can identify all dependencies in the backward direction and evaluate the impact of losing a facility, transport route, information services, or adequate input. In this way, there is less

likelihood of assigning scarce resources to obvious but non-critical items. One can develop a scenario assessment that involves criteria for evaluating severity, lead time, substitutability, and confidence in existing alternatives. The weights ought to reflect structured discussion rather than suggest mathematical accuracy. In the case of an ambiguous hazard, managers should make all necessary assumptions and consider different scenarios.

5.3. Performance Indicators and Learning Loops

Leading indicator categories could be the percentage of critical parts having validated sub-tier maps, percentage of alternate sources qualified, average time from alert to decision-making, number of critical routes having executable alternatives, and percentage of suppliers taking part in continuity exercises. Lagging indicators can be unmet orders, time taken for recovery, cost incurred on premium freight, margin compression, and loss of customers. Indicators must be broken down by region and criticality of the product.

It is clear that table 3 consciously avoids setting targets in terms of made-up benchmark figures. These must be set in relation to the company's service promises, the economics of the industry in which it operates, and its level of risk-taking. Nor should there be a focus on a single figure – cutting down decision-making time is useless if it leads to irrational or illegal decisions.

Table 3: Strategic Risk Management Scorecard for International Networks

Management dimension	Suggested indicator	Interpretation / decision use
Dependency transparency	Critical-tier mapping coverage (%)	Reveal hidden single points of failure
Response readiness	Qualified alternate capacity (%)	Check executable—not nominal—options
Decision speed	Alert-to-authorization time (hours)	Locate governance bottlenecks
Continuity	Critical-order fulfillment during shock (%)	Assess service protection
Recovery	Time to restore target throughput (days)	Track restoration trajectory
Adaptive renewal	Post-event mitigation actions closed (%)	Assess sustained learning

VI. DISCUSSION: STRATEGIC IMPLICATIONS FOR INTERNATIONAL BUSINESS

6.1. Network Advantage and the Limits of Firm-Level Optimization

This new framework will transform the managerial challenge from "How to make the company bounce back?" to "What are the interdependencies that have to stay intact for the business ecosystem to add value?" It will also force companies to think twice before making decisions about optimizing the process, which reduces cost in one entity at the expense of fragility of another one. The supplier that was forced to keep low inventory and to produce from only one factory could very well become the weak link of a very advanced buyer ecosystem. Risk management needs incentives for collective preparedness, not just liability transfer through contract management. Another important aspect of this new framework is the clarification of the relationship between visibility and control. Monitoring via technology will allow spotting delays or shortages; however, having knowledge will not provide us with capacity, alternative courses of action, or even governance.

6.2. Regionalization, Diversification, and Strategic Autonomy

Regionalization or nearshoring could cut down on transport distance and enhance monitoring capabilities, but would also result in concentration in one particular climatic region, labor market or regulatory regime. In contrast, dispersion of production activities geographically would decrease regional exposure but raise logistics complexity and costs of coordination. The right strategy would not consist in maximizing globalization or localization but in designing a system of dependencies that is consistent with service needs and possible risks of the organization. Autonomy as an element of corporate strategy should be understood as optionality, rather than self-sufficiency. Options can be preserved through alternative product specifications, pre-purchase of capacity, common tooling and explicit sub-tier contracting. This way of gaining flexibility does not require replication of all processes internally. But its economic rationale lies in disruption risk, benefits of continuity and costs of options.

6.3. Collaborative Risk Management and Trust

Sharing of information is hampered due to sensitivity issues, protection concerns and bargaining issues. The smaller suppliers might be hesitant to provide information on their capacity or supply chain links because they anticipate that it will be used for negotiating prices. Successful collaboration would entail provision of limited information for specific purposes, defined confidentiality agreements, mutual gains and emergencies response mechanisms. Trust cannot replace agreements and agreements cannot replace joint practice.

VII. IMPLEMENTATION ROADMAP FOR MANAGERS

7.1. Establish a Criticality-Based Baseline

The first cycle of implementation should determine what are the products, customer segments, and services whose disruption will have a disproportional impact. The organization can now identify its critical dependencies for achieving those objectives, including the latent logistics, software, financial, and certification dependencies. The risk management teams need to validate the critical dependencies with the operational and supplier teams and not only through procurement documentation.

7.2. Stress-Test the Network with Realistic Scenarios

The scenario workshop needs to encompass something more than just a case of supplier failure. Compound scenarios can be formed through a combination of a delay in transportation and a power disruption in the region, a cyber event with limited planning manually, or a policy limitation and concentration of suppliers. Participants need to determine the period of time available before exceeding the threshold of the service and find the first decision point that makes a difference to the result.

7.3. Fund a Diversified Response Portfolio

Interventions need to be compared according to their implementation costs, activation period, the scenarios under which they would work, and the dependencies that they create. There is some room for a buffer in the case of a component with a lengthy lead time, but capacity flexibility is needed where demand is highly variable. Alternative sources need to be qualified before any emergency and their ability to provide tools and data validated.

7.4. Institutionalizing Learning and Accountability

Post-disruption or exercise, teams will record the availability of signals, decision points, failed assumptions, and costs incurred. The measures to be undertaken will have accountability and deadlines attached. Lessons learned will involve reviewing supplier segmentation, risk tolerance levels, contract terms, and network design standards. Senior management will also assess if the resilience efforts actually decrease material exposure or just add reporting work.

VIII. LIMITATIONS AND FUTURE RESEARCH

However, there are several weaknesses associated with the study that need to be acknowledged while analyzing the developed framework. The first weakness is that the research uses conceptual synthesis, without conducting any empirical analysis and not generating any primary data. This implies that all five propositions presented in the paper can only be considered theoretically grounded expectations, and no causal relationships or effect sizes can be tested or established, nor the relative strengths of different resilience strategies quantitatively identified. It would be interesting for future research to empirically test these propositions using longitudinal disruptions data, multi-tier supply networks information, and operational performance measures in different firms and countries. Secondly, the framework takes the perspective of the lead firm as its unit of analysis. Such an approach may ignore the resource limitations, negotiating power asymmetries, and information exchange problems faced by small suppliers. Third, the literature synthesis is illustrative rather than exhaustive since the sources have been chosen based on their conceptual importance and complementarity rather than a registered systematic review procedure. While this makes theoretical integration easier, it may fail to account for all sector-based knowledge and conflicting information. A possible direction of future research is conducting a systematic review according to a clearly outlined methodology to test the validity and completeness of the suggested framework. Fourth, the applicability of the suggested strategies will depend on particular industry-related conditions. In highly regulated industries such as health care and aerospace, certification needs, product safety regulations, and qualification timeframes may prevent fast switching between suppliers. Hence, comparative studies by sector should analyze the effect of regulatory restrictions, product importance, and presence or absence of qualified substitutes on the success of resilience portfolios. Fifth, the framework has no quantitative analysis of the costs and benefits of redundancy, visibility, and regionalization. It should be examined in future research whether alternative strategies are financially and environmentally expensive, present cybersecurity risks due to increased data exchange, and how resilience costs should be distributed between the members of the network.

IX. CONCLUSION

Supply chain disruption on a global scale is a strategic management issue because the repercussions arise from networked dependencies and not independent risks. Firms operating internationally can protect themselves from such issues by being aware of which points in the system matter, how much the proposed solutions are real and not just nominal, and how their solution strategies are aligned with the actual mechanisms of shock transmission. This paper, drawn from the disciplines of network dependence, dynamic capabilities, and interorganizational

governance to present an integrated framework for strategic risk management. The integration results in three key implications. First, exposure is not equivalent to vulnerability; it is the substitutability, the coupling of the nodes and time to impact that define the repercussions of the shock. Second, digital visibility matters only if it allows coordinated actions. Third, resilience should be a portfolio of options and not just a preference for having more stock or more suppliers or shorter chains. This framework is not an empirical study that demonstrates improved performance. Rather, its significance lies in establishing testable relationships and defining practical steps that would serve as a starting point for future empirical studies. Business networks that operate internationally and view disruption management as a process of continuous learning and redesigning will likely be able to sustain crucial service provision and adjust to changing geopolitical, technological, and environmental conditions. The key contribution of the present study is development of the conceptual framework that brings together network dependency analysis, response portfolio selection, cross-organizational governance, and renewal after disruptions. It is important to note that resilience is not only about minimizing risk exposure and speeding up recovery, but also about sustaining feasible options, coordination of decision-making beyond organizational boundaries, and reduction of cyclical structural vulnerabilities. Still, it is yet to be seen how well these relationships work in practice and whether they can be generalized to other industries and institutions.

REFERENCES

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

[2] Habibi, F., Chakrabortty, R. K., & Abbasi, A. (2023). Evaluating supply chain network resilience considering disruption propagation. *Computers & Industrial Engineering*, *183*, 109531. https://doi.org/10.1016/j.cie.2023.109531

[3] Gaudenzi, B., Pellegrino, R., & Confente, I. (2023). Achieving supply chain resilience in an era of disruptions: a configuration approach of capacities and strategies. *Supply Chain Management: An International Journal*, *28*(7), 97-111. https://doi.org/10.1108/SCM-09-2022-0383

[4] Harju, A., Hallikas, J., Immonen, M., & Lintukangas, K. (2023). The impact of procurement digitalization on supply chain resilience: empirical evidence from Finland. *Supply Chain Management: An International Journal*, *28*(7), 62-76. https://doi.org/10.1108/SCM-08-2022-0312

[5] Petratos, P. N., & Faccia, A. (2023). Fake news, misinformation, disinformation and supply chain risks and disruptions: risk management and resilience using blockchain. *Annals of operations research*, *327*(2), 735-762. https://doi.org/10.1007/s10479-023-05242-4

[6] Cui, L., Wu, H., Wu, L., Kumar, A., & Tan, K. H. (2023). Investigating the relationship between digital technologies, supply chain integration and firm resilience in the context of COVID-19. *Annals of Operations Research*, *327*(2), 825-853. https://doi.org/10.1007/s10479-022-04735-y

[7] Yang, M., Lim, M. K., Qu, Y., Ni, D., & Xiao, Z. (2023). Supply chain risk management with machine learning technology: A literature review and future research directions. *Computers & Industrial Engineering*, *175*, 108859. https://doi.org/10.1016/j.cie.2022.108859

[8] Al Naimi, M., Faisal, M. N., Sobh, R., & Bin Sabir, L. (2022). A systematic mapping review exploring 10 years of research on supply chain resilience and reconfiguration. *International Journal of Logistics Research and Applications*, *25*(8), 1191-1218. https://doi.org/10.1080/13675567.2021.1893288

[9] Spieske, A., & Birkel, H. (2021). Improving supply chain resilience through industry 4.0: A systematic literature review under the impressions of the COVID-19 pandemic. *Computers & industrial engineering*, *158*, 107452. https://doi.org/10.1016/j.cie.2021.107452

[10] El Baz, J., & Ruel, S. (2021). Can supply chain risk management practices mitigate the disruption impacts on supply chains' resilience and robustness? Evidence from an empirical survey in a COVID-19 outbreak era. *International journal of production economics*, *233*, 107972. https://doi.org/10.1016/j.ijpe.2020.107972

[11] Miroudot, S. (2020). Resilience versus robustness in global value chains: Some policy implications. *COVID-19 and trade policy: Why turning inward won't work*, *2020*, 117-130.

[12] Naz, F., Kumar, A., Majumdar, A., & Agrawal, R. (2022). Is artificial intelligence an enabler of supply chain resiliency post COVID-19? An exploratory state-of-the-art review for future research. *Operations Management Research*, *15*(1), 378-398. https://doi.org/10.1007/s12063-021-00208-w

[13] Shishodia, A., Sharma, R., Rajesh, R., & Munim, Z. H. (2023). Supply chain resilience: A review, conceptual framework and future research. *The international journal of logistics management*, *34*(4), 879-908. https://doi.org/10.1108/IJLM-03-2021-0169

[14] Wulandhari, N. B. I., Budhwar, P., Mishra, N., Akbar, S., Do, Q., & Milligan, G. (2023). Organizational resilience to supply chain risks during the COVID-19 pandemic. *British Journal of Management*, *34*(3), 1282-1315. https://doi.org/10.1111/1467-8551.12648

[15] Liu, H., & Wei, S. (2022). Leveraging supply chain disruption orientation for resilience: the roles of supply chain risk management practices and analytics capability. *International Journal of Physical Distribution & Logistics Management*, *52*(9-10), 771-790. https://doi.org/10.1108/IJPDLM-04-2021-0135