Finance and Trade Dynamics
WISDOM ACADEMIC https://doi.org/10.63808/ftd.v2i3.493 Volume 2 , Issue 3

Conceptual Paper

From Tariffs to AI Fraud: The Evolution and Transmission Chains of New-Era Trade Risks in Cross-Border E-Commerce Clusters

Yingchun Yang[1], Nova C. Baldo[1,*]
[1]College of Business Administration, University of the Cordilleras, Baguio City 2600, Philippines
[*]**Correspondence:** Nova C. Baldo, ncbaldo@uc-bcf.edu.ph

Abstract

Cross-border e-commerce clusters bring together large numbers of small exporters using common platforms and logistics, but the various risks involved in these transactions, including volatile tariffs and carbon border taxation as well as fraud that takes place through generative artificial intelligence, are considered separately. This paper seeks to clarify how shocks from one type of risk can resurface in another and propagate within the cluster firms. Building upon the idea of risk contagion, the risk in the new era of international trade is identified as falling under three main families, their evolutionary pathways analyzed, and the results aggregated into a transmission chain model consisting of four components: risk source, coupling node, transmission path, and amplification condition. It is found that working capital and platform accounts are the key coupling points, while cluster density, shared infrastructure, and firm homogeneity are the factors that transform the shocks at the level of single firms into system-level risks.

Keywords

Cross-Border E-Commerce, Trade risk, Risk contagion, Industrial cluster, AI-Enabled Fraud

1. Introduction

Cross-border e-commerce has emerged as one of the most vibrant sectors within the realm of international business. Not only does the sector demonstrate growth in transactions and participation even amid challenging macroeconomic circumstances (Huo et al., 2024), but it creates externalities which go far beyond the borders of the participating businesses, boosting the vibrancy of entrepreneurship in cities where export-focused digital business takes place (Q. Yuan et al., 2024). Such clustering is not accidental. The way the sector functions forces small and medium-sized export companies to cluster geographically and

organizationally in order to use the same platforms and logistics systems and similar business models, thus reducing entry costs but making the participating companies equally dependent on the external environment.

The environment in which the clusters exist is now characterized not only by changes in its nature but also in its behavior. While tariffs were once relatively stable and predictable elements of trade, they now move along with changes in policy and have been supplemented with an increasing number of regulations in the field of environmental protection, namely carbon border adjustment. In addition to that, another set of risks has appeared, emerging directly from the digital space and consisting of the volatility of platform regulations and fraud due to generative artificial intelligence. The new kind of trade risk thus formed on two planes simultaneously on the plane of regulatory volatility and digitally-born threats and both converge right in the cluster.

Much research has been conducted on the different aspects of this landscape. Work on policy uncertainty, green barriers, risk associated with commerce through the platform, and digitally-enabled frauds has yielded verifiable results in its own way. Research into the structure of cross-border e-commerce ecosystem reveals much about it: its analysis shows that the factors that influence it are highly interdependent, and cannot be easily separated (Xi et al., 2023). There is one important implication of this result, which has not been addressed by the research that has led to it. If these factors are interdependent, the risks posed by them cannot be isolated either.

This is where the distinction comes in. Prior research deals with tariffs risks, business risks, and cybersecurity risks as independent fields of inquiry that involve different groups of researchers using different methodologies. The aspect of how these types of risks couple together and how shocks are horizontally transmitted through companies within a cluster where there are common platforms and similar organizational structures that facilitate this is relatively under-explored. A tariff risk evolving into a credit risk or a fraud risk turning into a fulfillment problem across many neighboring firms is not part of that analysis.

This study helps fill the gap with the aid of the risk contagion perspective. Specifically, the study creates a classification of three families of new era trade risk, examines the vertical development of each family, and then creates a holistic approach to analyzing transmission chains through four components: risk source, coupling node, transmission path, and amplification condition. The original contribution of the study is the creation of the holistic model of risk transmission analysis that answers why and how different risks spread through cluster networks. The rest of the study is organized in the order of typology, setting, vertical development, transmission chains, discussion, and conclusions.

WISDOM ACADEMIC https://doi.org/10.63808/ftd.v2i3.493 Volume 2 , Issue 3

2. New-Era Trade Risk and the Cluster Setting

2.1. A Three-Family Typology of New-Era Trade Risk

The risks associated with international online commerce are no longer suited to the existing typology of risk assessment for trade, which is based on a stable environment of tariffs and negotiated market access arrangements. An appropriate typology must be capable of dealing with two parallel changes: the changed nature of known risks in the new environment and the emergence of risks that do not exist in a pre-digitized world. Recent studies of the issue of security risks in the digital economy show that there are different kinds of regulatory, transactional, and data risks, and each one requires a separate approach in governance (S. Wang et al., 2025).

Extending this logic of differentiation, the framework identifies three categories of risk. First, there is policy and green-regulatory risk, which encompasses risk from tariffs, trade policy, and the increasingly wide-ranging array of green regulation that puts sustainability criteria on market access. Second, there is traditional commercial risk, but digitalized, or risk that involves credit, fulfillment, and logistical issues but was already an issue prior to e-commerce and has since been reframed through platform mediation. Third, there is digitally-native risk, which involves those risks that would not exist without digital technology, such as platform rule risk, data risk, and AI-enabled fraud. As seen in Table 1 below, there is a distinct way in which each of the three categories manifests itself at the level of the cluster, and the three risk categories organize the vertical analysis in Section 3.

The typology has an analytical role that goes beyond mere classification. It is precisely because the conceptual separation of the families is maintained here that their subsequent pairing becomes noticeable: interfamily transfer can only become clear if the demarcation between the families is first made precise.

Table 1

A Three-Family Typology of New-Era Trade Risk in Cross-Border E-Commerce Clusters

Risk family	Representative forms	Cluster-level manifestation
Policy and green-regulatory risk	Tariff volatility; unilateral trade measures; carbon border adjustment; green technical barriers	Compliance cost surges pressing on densely clustered SME exporters
Traditional commercial risk in digital form	Credit and financing risk; fulfillment risk; logistics and operational disruption	Account freezes, platform payment risk, logistics data risk under platform dependence
Digitally native risk	Platform rule volatility; data security breaches; AI-enabled fraud such as	High-frequency information and transaction flows enlarging

2.2. Cross-Border E-Commerce Clusters as the Unit of Analysis

The correct unit to examine the interactions of these families of risks is not the firm but the cluster itself, as there are three factors that govern the process of contagion in cross-border e-commerce clusters, and they relate to the structure of the cluster. First, it is a dense concentration of small and medium-sized firms. Clusters tend to bring together a significant number of undercapitalized exporting firms in a relatively small physical and institutional space, where any disturbance capable of impacting one firm can impact many others in its vicinity.

The second aspect is shared infrastructure. Most of the business dealings such as sale and transactions happen over a few digital platforms for the cluster companies, and findings regarding performance from the platform have shown that the platform acts as an operational infrastructure rather than just being the sales avenue (Yang et al., 2023). The reliance of the firms on the platform happens along the downstream side because the effectiveness of the supply chain in cross-border e-commerce depends on shared logistics and warehousing infrastructure that focuses the physical delivery of the cluster businesses in a common corridor (K. Yuan et al., 2025). The shared infrastructure saves costs precisely by concentrating exposure at common nodes, an effect that remains hidden until such a node is under strain.

The third characteristic is homogeneity of structure. The companies in the cluster end up having very similar technology platforms, product strategy, and work processes, an effect that gets reinforced by the discovery that cross-border e-commerce development creates a systematic push toward similar paths of digital technology adoption among the companies (K. Chen & Luo, 2024). Homogeneity is interpreted as an indicator of maturity for the cluster. In terms of risk, this indicates that companies not only have a similar infrastructure but also have similar vulnerabilities; a shock that works against one company works against all the others in the cluster.

All in all, density provides the point of contact, infrastructure provides the conduit, and homogeneity provides the vulnerability. The three characteristics create the substrate for the horizontal transmission discussed in Section 4.

2.3. A Risk-Contagion Lens on Trade Risk

An explanation for how the shock to one risk family manifests itself as damage in another needs the conceptual language that does not exist in the field of trade policy analysis.

This concept has been articulated by contagion theory in risk, mostly in the fields of finance and network economics. The basic claim of this theory is that risks spread due to links between entities exposed to them, and that the structure of these links, as opposed to the size of the shock alone, dictates the end size of the damage caused. Network based measures have shown that contagion power between two related industries can be measured and tracked along defined linkages (Hu & Guo, 2024).

There are two contagion-related streams of research that are significant for the cluster environment. Credit risk contagion studies in supply chain financing have demonstrated that financial stress spreads through operational relations, turning liquidity problems of the counterparty into an own default risk, which provides the basis for the mechanism of contagion shocks from the commercial world to the financial position of adjacent firms (W. Chen et al., 2021). In addition to the one-dimensional view of contagion, research into risk transmission under the influence of multiple drivers has proven that, if several factors of risk affect the system at once, their combined influence results in effects that cannot be achieved by means of single-factor models (J. Wang et al., 2021). The multi-driver result is directly relevant here, because cluster firms face policy, commercial, and digital shocks concurrently rather than sequentially.

In relation to the current case, the contagion perspective redefines the three families of risks mentioned above as sources of contagion, and the three cluster characteristics as conditions of the network that determine the propagation process. Section 4 translates the aforementioned into transmission paths.

3. The Vertical Evolution of Each Risk Family

3.1. From Static Tariffs to Volatile Policy and Green Barriers

In the first group of risks, what has changed is not the amount of trade barriers but how they change over time. As long as under the multilateral regime that governed trade during the late twentieth century, tariffs were stable parameters that could be incorporated into pricing years ahead for exporting companies, the dynamics of trade has changed significantly. As research on economic policy uncertainty indicates, changes in the political climate negatively affect exports through having a depressive impact, indicating that economic policy uncertainty became an additional cost channel and not simply the background (Liu et al., 2024). There are more fundamental changes in behavior as well. For instance, evidence from listed industrial exporters proves that trade policy uncertainty leads to a transformation of exporting strategies as companies prepare for non-existent barriers to trade (Zhou & Wen,

2022). It is quite a new type of risk, considering that damage here is caused not by increased costs of exporting but by distortions in behavior of firms.

In addition to all these uncertainties, the family has developed yet another new branch - green regulations. The carbon border adjustment mechanism of the European Union is the prime example of such an instrument and analysis of how it works proves its capability to reduce the incidence of carbon leakage (Lan & Tao, 2024). In terms of the export market, such a reduction is implemented in the form of compliance requirement. The trade impacts of green barriers have been observed in particular industries. Photovoltaic exports to the ASEAN region have been subjected to an inhibition caused by green trade barriers, which is quite indicative as it reveals how environmental policies limit production of the very type of goods they are supposed to encourage (S. Chen, 2024). The effect of regulatory pressure is not necessarily negative; indeed, firms facing green barriers in an environment characterized by favorable national policies have been shown to innovate greener technologies (Xu et al., 2024). However, such adaptation depends upon resources that are lacking amongst the firms in the clusters. There are high fixed costs associated with carbon accounting, certification, and process changes. When fixed costs of regulatory compliance are imposed on a group of small, undercapitalized firms, then fixed costs as a percentage of revenue increase as the size of the firm decreases.

3.2. The Digitalization of Traditional Credit and Operational Risk

The second group of risks presents nothing new categorically speaking. Credit risk, risk of non-fulfillment, and risk of logistics disruptions existed since long-distance trade emerged. But what has changed is how these risks operate. Platform mediation has moved the levers, shrunk the timelines, and modified the assets at which these risks are aimed. Credit risk demonstrates how that happened. Whereas in classical trade credit risk was gauged using the banking channel and documents, in platform-based trade credit risk is embedded in account status, transaction history, and payments conducted via platform. Analysis of bonded warehouse schemes demonstrates that in cross-border e-commerce financing is now contingent on information produced by logistics and platform systems themselves and inventory visibility replaces collateral analysis (Song et al., 2024). But the process goes the other way around as well. When credit risk is determined by the information created by the platform, any disruption of the latter, account freezing, payment suspensions, information discrepancies become credit risk events regardless of the firm’s financial position.

Risk at the operational and logistics level has also been transformed alongside. Evidence from field experiments with the introduction of blockchain into cross-border trade shows that

increased efficiency is the result of the digitization of documentation and authentication processes, which provides proof that the operational layer of trade itself has become an information system (Tian et al., 2024). This proof also comes with a reverse side of the coin that is ignored by studies of efficiency – processes that become more efficient through digitization become vulnerable through digitization too. Corrupted information flows or synchronization problems will stop the process of fulfillment just as much as the closure of a port would. Cluster firms operate in platforms and logistics that are shared between them, making the practical interpretation of commercial risk shift from physical to informational disruptions, while risks of credit, fulfillment, and delivery are still easily recognizable.

3.3. AI-Enabled Fraud as the Frontier of Digitally-Native Risk

The third family is different from the second in kind rather than in degree. Digital-born risks are not just the old risks in a new guise but dangers whose very presence relies on digital infrastructure. In the third family, the danger of AI-enabled fraud represents today's cutting edge. The systematic study of deepfakes in business contexts has shown that synthetic media have graduated from being a novelty to becoming a tool of business fraud, one able to create the identification signals upon which business relies (Mustak et al., 2023). The threat profile has two key features. The first is the capacity for deception: an analysis of generative AI in social engineering reveals that machine-generated deception is as persuasive as human-generated deception while being producible at minimal marginal cost, which overwhelms screening systems optimized for human-scale levels of fraud (Schmitt & Flechais, 2024). The second is organizational scale. Qualitative analysis of bank executives reveals that deepfake attacks put organizations at risk of operational disruption, not just financial transactions, because one deepfake impersonation could jeopardize both authorization and counterparty verification in one stroke (Vecchietti et al., 2025).

The clustering context accentuates both characteristics. Transactions involving cross-border e-commerce are conducted through frequent but small transactions among unknown parties, and these transactions require digital identification proof in terms of the very same signals that generative techniques currently produce. Research into identity fraud involving account credentials in online platform ecosystems acknowledges the fact that account credentials are an integral part of the attack surface and are used on a large scale wherever transaction volume precludes individual inspection (Chang et al., 2023). Large volume is one of the most prominent features of the cluster context. Fraud technique that operates on the basis of high transaction volume and light verification therefore fits into the clustering context as its optimal setting: thousands of similar companies making continuous

transactions on common platforms, and each individual transaction being too small to afford the necessary verification.

4. Horizontal Transmission Chains within the Cluster

4.1. Cross-Family Coupling Mechanisms

This is where the contagion perspective from Section 2.3 starts taking effect once the coupling points between the various risk families are identified. The coupling point is any situation whereby a single asset or activity assumes responsibility for more than one risk family at the same time so that any event affecting one risk family cannot fail to have an effect on all the others. The modeling of risk transmission in international supply chains demonstrates this basic concept: risk states flow between organizations via the operational connections that exist among organizations, and effective control mechanisms can only work if they focus on the connection itself rather than on the initial shock (Lei et al., 2021). Applied within the firm rather than between firms, the same principle identifies which internal assets function as inter-family bridges.

Two couplings are prevalent in the cluster environment. The first coupling stretches from the policy domain into the business domain via the cash flow status of the company. When the green-regulatory shock occurs, it happens as a regulatory requirement, but for an undercapitalized exporting company, the cost incurred by compliance and the profit made from the exports rely on the same working capital. Thus, the regulatory cost becomes the liquidity issue that is interpreted as lower creditworthiness by credit platforms, whereas certification delays result in a logistic risk as the goods get stuck at the borders. One policy event thus triggers compliance, credit, and logistics risk simultaneously, not because the categories are confused but because a single balance sheet carries all three exposures.

The second pairing moves from the digitally native family to the commercial family via the platform account. As was seen in Section 3.2, account status is now synonymous with credit rating, while account credentials are now the primary targets of fraud enabled by artificial intelligence, as seen in Section 3.3. The point where the two intersect serves as the coupling point. In the case of either an actual or suspected instance of fraud, account freezes and payment suspensions are instituted. These actions isolate the payment process and the order data flow of the business simultaneously; and since in-process fulfillment relies on the data flow for both the settlement and shipping instructions, the disruption soon cascades to physical fulfillment operations.

4.2. Amplification through Cluster Density and Platform Dependence

Coupling is the reason why risk becomes inter-family within an organization, while amplification is the reason why the risk moves beyond the organization to other organizations. The three cluster characteristics described in Section 2.2 function as multipliers in this scenario. Simulations of network structures in supply chains prove this point structurally: networks with high levels of clustering coefficients display lower resilience in the process of risk propagation, which implies that being highly interconnected, i.e., the very essence of clustering, is a risk-transmission problem (Xue et al., 2024). Density converts a coupled shock in one firm into simultaneous exposure for its many neighbors.

The dependence of the company on the platform is the second multiplier. Platform dependence entrepreneurship shows that companies which work within the dominant platform have a structurally asymmetric power relationship because they cannot affect the laws, algorithms, and enforcement measures regulating their business activities (Cutolo & Kenney, 2021). From the point of view of risks, the term “asymmetry” suggests that defensive mechanisms, increased regulation, general inspection of the accounts, payment blocking – these all are implemented on groups of sellers rather than individuals who committed some mistakes. The fraud carried out by one company triggers enforcement measures against other companies similar to this one. Amplification has identifiable trigger conditions: it activates when the coupled shock touches a shared node, when the affected firm profile is common within the cluster, and when the platform or logistics response operates at category rather than firm granularity. Where none of these conditions holds, a coupled shock remains a private misfortune; where all three hold, it becomes systemic.

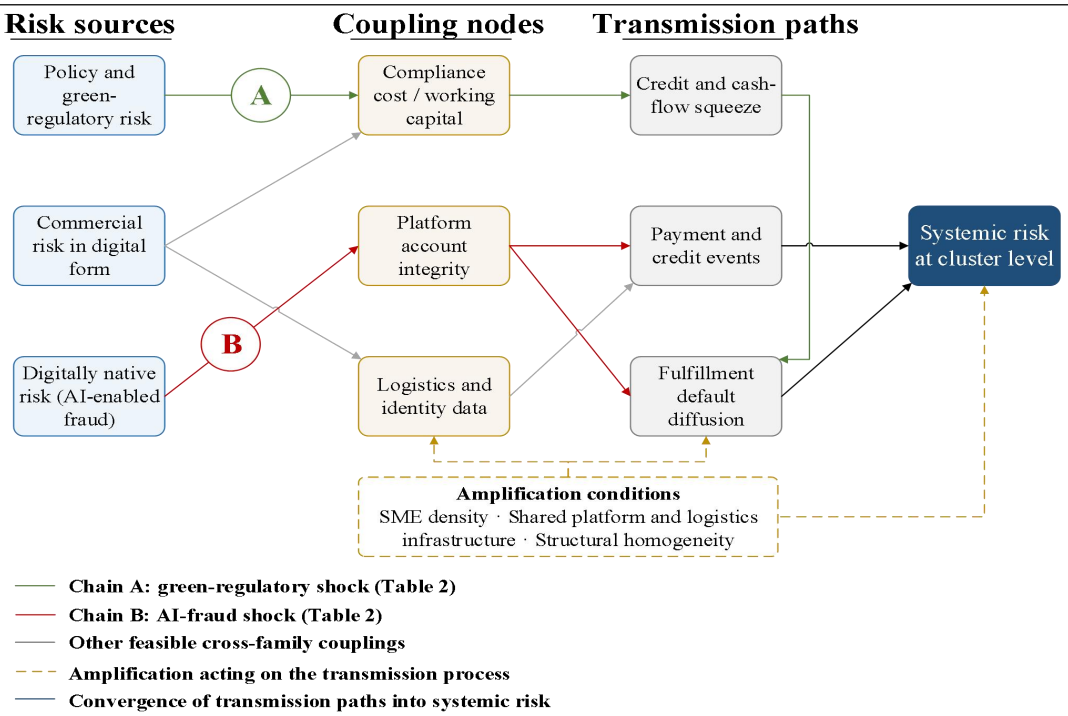
4.3. An Integrated Framework and Illustrative Transmission Chains

This constitutes a framework consisting of four components: risk source, coupling node, transmission path, and amplification condition. A risk source is a shock that arises in any of the three groups; the coupling node is the asset by which the shock passes between the two families; the transmission path is the chain of states in which the damage travels; and the amplification condition is the set of group characteristics by which the transmission of damage rises from the firm level to the system level. As depicted in Figure 1 below, the framework allows for the shock source and coupling point to be any combination of each other.

Figure 1

Cross-family risk transmission framework in cross-border e-commerce clusters

Finance and Trade Dynamics
WISDOM ACADEMIC https://doi.org/10.63808/ftd.v2i3.493 Volume 2 , Issue 3



Two named chains demonstrate how the model works from end to end, as seen in Table 2 below. Chain A starts from the green regulation domain where a carbon border adjustment shock increases the compliance cost, which in turn reduces credit and cash flows, and the fulfillment default ripples throughout the cluster because neighbors with identical exposure face the same limitation. Chain B starts from the AI-based fraud domain where a deepfake identity attack undermines the integrity of accounts on the platform, which in turn triggers credit events and disrupts logistics instructions, and category-wide enforcement causes harm to firms without any fraud at all. Empirical observation of trade networks supports the realism of such end-to-end sequences, with shock transmission through China's corn import network demonstrating that disturbances entering at one node propagate through identifiable paths across the network (Wu & Zhu, 2025). The two chains differ in origin but converge on the same terminal state, systemic fulfillment and credit deterioration, which is the framework's central claim in compact form: heterogeneous sources, homogeneous outcomes, connected by the cluster's own architecture.

Table 2

Two Illustrative Transmission Chains Decomposed by Framework Element

Chain	Risk source	Coupling node	Transmission path → cluster outcome
A: Green-regulatory	Carbon border adjustment shock	Compliance cost surge	Credit and cash-flow squeeze → fulfillment defaults diffusing across the cluster
B: AI-fraud	Deepfake identity incident	Platform account integrity	Account freezes and payment suspension → credit events and logistics interruption spreading to similarly profiled firms

Note. *Amplification conditions (SME density, shared platform and logistics infrastructure, structural homogeneity) apply to both chains.*

5. Discussion

This framework's main finding—that different risk sources produce similar results at a homogenous level via identifiable coupling nodes—has an immediate implication for the design of a governance structure. Current governance of risk management in cross-border e-commerce is fragmented into categories, with customs compliance groups managing policy risk, service providers managing account risk, and anti-fraud measures managing deception. This framework shows why such an arrangement will not work effectively. Controls will be set up at risk sources, yet as the analysis in Section 4 indicates, the critical step happens at coupling nodes and conditions of amplification, which cannot be observed from any one category-specific instrument. Defenses established solely at the sources will be perfectly adequate at each source point and yet fail to deliver system-wide success because failure is located outside the categories.

This comparison with surrounding literature strengthens the above reading even further. Even in the context of cutting-edge defensive technologies, the issue of detection in the context of deepfakes admits of a continual arms race with generative capacity being matched with every innovation made in detection capacities (Singh et al., 2025). If such defenses at the source are themselves only provisionally defensible even in the most favorable circumstances, the weight of governance must be shifted to the couplings and insulating the operational working capital and fulfillment processes from such compliance shocks. Indeed, empirical literature suggests the same direction in the case of resilience in SMEs; firms able to navigate the recent disruptions have done so using adaptation of their operation and digital capability structures (Fodouop Kouam, 2025). Adaptation operates on the firm's internal linkages, which is precisely where the framework locates transmission, and the two findings therefore point in the same direction as the framework rather than merely coexisting with it.

However, the validity of the framework is conditional. The mechanisms of the framework rely on the three structural attributes of Section 2.2, and in places where these attributes are diminished, so too will the transmission be diminished. The dependence mechanism has a non-linear relationship; research into seller platform dependence has revealed that there is a U-shaped relationship between seller platform dependence and its outcome, depending on whether the seller is a new entrant to the market or a more established firm, as well as the size of the seller (Ju et al., 2025). This shows that the mechanisms of

Section 4.2 apply in a stronger fashion to small clusters of sellers using dominant platforms, as opposed to large sellers who are multi-homed or use differentiated logistics.

Two limitations arise from the nature of the study's approach. First, being an exercise in literature-based synthesis, the model is based not on the observation of transmission but on the plausibility of mechanisms and cross-domain analogies, and the contagion data used comes from the supply chain, finance, and agricultural trade systems, not from e-commerce clusters. The illustrative chains, although internally consistent, are still analytical models. These limitations may be addressed by future research efforts, such as the examination of recorded account freeze or compliance shock incidents through cluster transaction records, transforming the models into empirically tested propositions. Comparative study of clusters that vary in their degree of platform reliance will help define the boundary conditions for the analysis.

6. Conclusion

In this paper, it was attempted to show how trade risks coming from different fields, such as tariff variability and artificial intelligence frauds, cause a similar kind of harm within cross-border e-commerce clusters. The analysis is based on the three-family classification of new era trade risks along with a risk contagion model of the structure of the cluster, wherein the vertical development of each family was followed, and then all were brought together horizontally to create the four components of the model, namely risk source, coupling node, transmission pathway, and amplification condition. The two named examples of transmission chain, one being regulatory and other fraud-induced, proved that the framework is a continuous process wherein shocks spread across different families through shared resources.

The contribution is an integrated analytical framework for a risk environment that existing studies analyze in pieces. In the realm of SME risk management, the framework realigns focus from specialized strategies to points of interaction where the cross-family transformation of risks is taking place; a move that can be achieved by thinly capitalized cluster companies by means of liquidity buffers and fulfillment insulation. From an academic standpoint, the two processes serve as testable theories; transactional data from account freezing and compliance shock events provide a direct way forward from this framework to its validation.

Acknowledgments

Not applicable.

Author contributions

Not applicable.

Funding

This research received no external funding.

Data availability

No datasets were generated or analysed during the current study.

Declarations

Conflict of interest

The authors declare that there is no conflict of interest.

Ethics approval

Not applicable.

Consent to participate

Not applicable.

Consent for publication

All authors have given their consent.

Publisher's Note

Wisdom Academic Press Ltd. remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

[1] Huo, D., Ouyang, R., Tang, A., Gu, W., & Liu, Z. (2024). New growth in cross-border e-business: Evidence from gray forecasting to cross-border e-business in China. *Journal of Internet and Digital Economics*, *4*(1), 12-29.

[2] Yuan, Q., Ji, Y., Zhang, W., & Lei, T. (2024). Cross-border e-commerce and urban entrepreneurial vitality: A quasi-natural experiment evidence from China. *Sustainability*, *16*(5), 1802.

[3] Xi, X., Wei, M., & Teo, B. S. X. (2023). Analysis of the key influencing factors of China's cross-border e-commerce ecosystem based on the DEMATEL-ISM method. *PLOS ONE*, *18*(8), e0287401.

[4] Wang, S., Liu, H., Li, Z., & Zhang, S. (2025). Security risks and regulation of cross-border e-commerce in digital economy. *Journal of Electronic Business & Digital Economics*, *4*(2), 385-401.

[5] Yang, Y., Chen, N., & Chen, H. (2023). The digital platform, enterprise digital transformation, and enterprise performance of cross-border e-commerce: From the perspective of digital transformation and data elements. *Journal of Theoretical and Applied Electronic Commerce Research*, *18*(2), 777-794.

[6] Yuan, K., Zhang, C., Hou, R., & Gao, X. (2025). Can cross-border e-commerce development improve supply chain efficiency? Empirical evidence from China. *Applied Economics*, *57*(56), 9606-9622.

[7] Chen, K., & Luo, S. (2024). Cross border e-commerce development and enterprise digital technology innovation: Empirical evidence from listed companies in China. *Heliyon*, *10*(15).

[8] Hu, C., & Guo, R. (2024). Research on risk contagion in ESG industries: An information entropy-based network approach. *Entropy*, *26*(3), 206.

[9] Chen, W., Li, Z., & Xiao, Z. (2021). On credit risk contagion of supply chain finance under COVID-19. *Journal of Mathematics*, *2021*(1), 1281825.

[10] Wang, J., Zhou, H., & Jin, X. (2021). Risk transmission in complex supply chain network with multi-drivers. *Chaos, Solitons & Fractals*, *143*, 110259.

[11] Liu, D., Zhu, X., & Yu, H. (2024). Economic policy uncertainty, intra-industry trade, and China's mechanical and electrical product exports. *PLOS ONE*, *19*(1), e0290866.

[12] Zhou, F., & Wen, H. (2022). Trade policy uncertainty, development strategy, and export behavior: Evidence from listed industrial companies in China. *Journal of Asian Economics*, *82*, 101528.

[13] Lan, T., & Tao, R. (2024). Research on the inhibitory effect of the EU's carbon border adjustment mechanism on carbon leakage. *Sustainability*, *16*(17), 7429.

[14] Chen, S. (2024). The impact of green trade barriers on China's photovoltaic products exports to ASEAN. *Frontiers in Environmental Science*, *12*, 1459950.

[15] Xu, P., Jin, Z., & Wu, X. (2024). Effect of green trade barriers on export enterprise green technological innovation from the perspective of the low-carbon city pilot policy. *Frontiers in Environmental Science*, *12*, 1486855.

[16] Song, L., Chen, Y., Zhang, B., & Zhu, M. (2024). Inventory and financing decisions in cross-border e-commerce: The financing and information roles of a bonded warehouse. *Expert Systems with Applications*, *238*, 121639.

[17] Tian, X., Zhu, J., Zhao, X., & Wu, J. (2024). Improving operational efficiency through blockchain: Evidence from a field experiment in cross-border trade. *Production Planning & Control*, *35*(9), 1009-1024.

[18] Mustak, M., Salminen, J., Mäntymäki, M., Rahman, A., & Dwivedi, Y. K. (2023). Deepfakes: Deceptions, mitigations, and opportunities. *Journal of Business Research*, *154*, 113368.

[19] Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, *57*(12), 324.

[20] Vecchietti, G., Liyanaarachchi, G., & Viglia, G. (2025). Managing deepfakes with artificial intelligence: Introducing the business privacy calculus. *Journal of Business Research*, *186*, 115010.

[21] Chang, Y. W., Shih, H. Y., & Lin, T. N. (2023). AI-URG: Account identity-based uncertain graph framework for fraud detection. *IEEE Transactions on Computational Social Systems*, *11*(3), 3706-3728.

[22] Lei, Z., Lim, M. K., Cui, L., & Wang, Y. (2021). Modelling of risk transmission and control strategy in the transnational supply chain. *International Journal of Production Research*, *59*(1), 148-167.

[23] Xue, S., Li, J., Yu, J., Li, M., & Shi, X. (2024). Research on supply chain network resilience: Considering risk propagation and node type. *Applied Sciences*, *14*(7), 2675.

[24] Cutolo, D., & Kenney, M. (2021). Platform-dependent entrepreneurs: Power asymmetries, risks, and strategies in the platform economy. *Academy of Management Perspectives*, *35*(4), 584-605.

[25] Wu, J., & Zhu, J. (2025). Risk transmission and resilience of China's corn import trade network. *Foods*, *14*(8), 1401.

[26] Singh, L. H., Charanarur, P., & Chaudhary, N. K. (2025). Advancements in detecting deepfakes: AI algorithms and future prospects: A review. *Discover Internet of Things*, *5*(1), 53.

[27] Fodouop Kouam, A. W. (2025). Navigating disruption: The role of resilience and digital transformation in Chinese cross-border e-commerce SMEs post-COVID-19. *SAGE Open*, *15*(4), 21582440251405028.

[28] Ju, C., Guo, Q., Jiang, H., & Wang, Y. (2025). Does platform dependence always reduce the fairness perception of seller? *Electronic Markets*, *35*(1), 51.