



International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Integrating Geopolitical, Cybersecurity, and Operational Signals for Dynamic Third-Party Risk Intelligence in United States Supply Chains

Igbinabor Okunbor

Delta State University, Nigeria

DOI : <https://doi.org/10.55248/gengpi.07.0926.2921>

ABSTRACT :

United States supply chains increasingly depend on globally distributed networks of manufacturers, logistics providers, technology vendors, cloud platforms, and specialized service organizations, creating interconnected exposures that conventional third-party risk assessments may inadequately capture. Geopolitical instability, cyber threats, operational disruption, trade restrictions, infrastructure failures, and supplier concentration can interact dynamically, transforming localized vulnerabilities into cascading supply-chain consequences. This study develops an integrated framework for dynamic third-party risk intelligence by combining geopolitical, cybersecurity, operational, transactional, and supplier-dependency signals within a unified predictive environment. Temporal analytics and machine-learning techniques are applied to identify emerging deterioration, anomalous behaviour, persistent risk patterns, and cross-domain interactions before significant disruption materializes. The framework incorporates supplier-specific baselines, dependency mapping, explainable risk attribution, prediction confidence, and continuously updated composite risk scores to support differentiated early-warning classifications. Risk intelligence is subsequently connected with proactive interventions including supplier engagement, inventory protection, alternative sourcing, cybersecurity escalation, and continuity activation. The proposed approach advances third-party risk management from periodic, domain-specific assessment toward integrated, forward-looking intelligence capable of strengthening operational resilience across complex United States supply networks.

Keywords: Third-Party Risk Intelligence; Geopolitical Risk; Cybersecurity Analytics; Supply Chain Resilience; Machine Learning; Predictive Risk Analytics

1. INTRODUCTION

1.1 Expanding Third-Party Exposure Across United States Supply Chains

United States supply chains increasingly operate through globally distributed ecosystems of manufacturers, component suppliers, logistics providers, technology vendors, cloud platforms, contractors, and specialized service organizations [1]. Outsourcing and digital integration have expanded access to specialized capabilities while simultaneously increasing organizational dependence on entities beyond direct managerial control. Lean sourcing structures and geographically dispersed production can further reduce the buffers available when external partners experience disruption [2]. A failure affecting one strategically positioned third party may propagate through shared production, transportation, technology, or service dependencies, influencing organizations that have no direct relationship with the originating entity [3]. Multi-tier sourcing intensifies this exposure because direct suppliers frequently depend on upstream organizations with limited buyer visibility [4]. Third-party exposure must therefore be understood as a networked resilience challenge affecting procurement continuity, production availability, digital operations, logistics performance, and downstream customer fulfilment [5].

1.2 Convergence of Geopolitical, Cybersecurity, and Operational Risk

Contemporary third-party disruptions increasingly develop through interactions among geopolitical, cybersecurity, and operational conditions rather than within isolated risk domains [2]. Regional conflict, sanctions, export restrictions, or trade-policy changes can constrain materials and transportation routes while simultaneously altering cyber-threat exposure [6]. Rapid supplier substitution following geopolitical disruption may also introduce unfamiliar digital connections, service providers, and operational dependencies. Conversely, ransomware, software compromise, or infrastructure attacks affecting suppliers, logistics platforms, ports, or technology providers can translate digital incidents directly into physical production and distribution interruptions [7]. Energy shortages, telecommunications failures, supplier outages, and transportation instability can further amplify these effects. Consequently, individually manageable vulnerabilities may become substantially more disruptive when they interact through common suppliers, infrastructure, technologies, or geographic dependencies [4].

1.3 Limitations of Siloed and Periodic Third-Party Risk Assessment

Traditional third-party oversight commonly separates risk into specialized assessment processes. Procurement functions may use supplier questionnaires and operational scorecards, while cybersecurity teams conduct security assessments and enterprise-risk functions monitor geopolitical or compliance exposure [3]. Although useful independently, these mechanisms can create fragmented representations of supplier vulnerability when information remains separated across organizational functions [7]. Periodic audits and static vendor classifications may also become outdated between assessment cycles as cyber threats, geopolitical conditions, and supplier performance evolve. More importantly, isolated thresholds can overlook weak but correlated deterioration signals [5]. A minor operational delay, emerging cyber vulnerability, and increasing regional instability may appear insignificant independently but collectively indicate substantially greater exposure [9]. Effective early warning therefore requires cross-domain intelligence rather than parallel risk monitoring.

1.4 Aim, Scope, and Contribution

This article develops an integrated analytical framework for dynamic third-party risk intelligence across United States supply chains. It combines geopolitical indicators, cybersecurity telemetry, operational performance, commercial behaviour, and supplier-dependency information within a temporally synchronized analytical environment [4]. Machine-learning prediction and anomaly detection are employed to identify deterioration trajectories, abnormal supplier behaviour, and compound risk patterns before significant disruption materializes [6]. The framework extends beyond probability estimation by incorporating supplier criticality, network dependency, substitutability, deterioration persistence, and prediction confidence into dynamic prioritization. Explainable risk attribution identifies the specific geopolitical, cybersecurity, and operational signals responsible for changing supplier classifications [8]. These outputs subsequently inform differentiated interventions including supplier engagement, cybersecurity escalation, alternative sourcing, inventory protection, logistics adjustment, and continuity activation connecting predictive intelligence directly with proactive supply-chain resilience [9].

2. CONCEPTUAL FOUNDATIONS OF INTEGRATED THIRD-PARTY RISK INTELLIGENCE

2.1 Evolution From Vendor Assessment to Dynamic Third-Party Risk Management

Third-party risk management has evolved from supplier qualification and periodic compliance verification toward continuous monitoring of interconnected external dependencies [7]. Traditional vendor assessment concentrated primarily on contractual capability, financial stability, quality, and regulatory compliance. Globalization and extensive outsourcing subsequently expanded organizational exposure to geographically dispersed suppliers and service providers operating across multiple jurisdictions [10]. Digital transformation has further connected third parties through cloud platforms, enterprise applications, APIs, shared data environments, and remote-access infrastructure. These relationships create dependencies that extend beyond physical supply continuity into cybersecurity and digital-service availability [13]. Multi-tier sourcing compounds this complexity because direct suppliers may depend on upstream manufacturers, technology providers, or infrastructure operators that remain outside buyer visibility [8]. Consequently, contemporary third-party risk management increasingly requires continuous intelligence capable of monitoring changing vulnerabilities across both physical and digital supply networks.

2.2 Geopolitical Risk and Supply-Network Exposure

Geopolitical conditions can alter supplier accessibility, cost structures, transportation reliability, and continuity with limited warning [9]. Sanctions and export controls may restrict transactions with particular organizations, technologies, commodities, or jurisdictions, while tariffs can change sourcing economics and supplier competitiveness. Armed conflict and political instability may interrupt production facilities, energy infrastructure, ports, border crossings, or established transportation corridors [12]. Regulatory divergence can additionally increase compliance complexity for suppliers operating across multiple markets. Strategic-resource concentration creates further vulnerability where essential minerals, components, energy resources, or manufacturing capabilities originate from a limited geographic area [15]. Geographic exposure should therefore be analysed alongside supplier relationships and logistics dependencies rather than treated simply as country-level risk [7]. A supplier located outside an affected region may remain materially exposed through upstream production, transportation routes, critical inputs, or facilities concentrated within geopolitically vulnerable locations.

2.3 Cybersecurity Risk Across Digitally Connected Third Parties

Digitally integrated supply chains create attack surfaces extending beyond an organization's internal security perimeter [11]. Suppliers may access corporate systems through credentials, APIs, cloud environments, software integrations, managed services, and remote administration channels. Credential compromise or exploitation of unpatched vulnerabilities can therefore allow attackers to exploit trusted third-party relationships [14]. Ransomware affecting a supplier can also interrupt production, order processing, transportation coordination, or digital services even when the purchasing organization is not directly compromised. Software supply-chain attacks create additional exposure when malicious code or compromised updates propagate through widely used applications [8]. Cloud-service concentration further means that disruption at a shared technology provider can affect numerous interconnected organizations simultaneously [13]. Cybersecurity risk intelligence must consequently evaluate both the probability of compromise and the operational importance of the digital services, data flows, and access relationships associated with each third party.

2.4 Operational Risk and Disruption Propagation

Operational deterioration frequently provides observable evidence that a supplier's ability to maintain expected service is weakening [10]. Capacity constraints, equipment downtime, workforce shortages, declining quality, and production instability can reduce available output, while lead-time volatility and transportation delays can disrupt scheduled material flows. Infrastructure outages affecting electricity, telecommunications, ports, or transportation networks may create additional constraints beyond the supplier's direct control [15]. These conditions can manifest downstream through incomplete deliveries, inventory shortages, production rescheduling, customer delays, and service degradation [9]. Propagation becomes particularly severe where buyers maintain limited safety stock, depend on single-source suppliers, or require lengthy qualification periods for substitutes. Shared suppliers and logistics infrastructure can additionally transmit one localized disruption across several facilities or product lines [12]. Operational risk must therefore be assessed in relation to both deterioration severity and the network pathways through which disruption can spread.

2.5 Cross-Domain Risk Interaction and Analytical Gap

Geopolitical, cybersecurity, and operational risks can interact in ways that make independent assessment analytically incomplete [8]. Regional conflict, for example, may disrupt energy availability and transportation while simultaneously increasing cyber-threat activity against organizations associated with affected countries or strategic sectors [14]. Trade restrictions may force rapid supplier substitution, creating new operational dependencies and digital connections that have not undergone equivalent risk assessment. Similarly, a cyberattack against a logistics or infrastructure provider can transform a digital compromise into physical transportation and inventory disruption [11]. Conventional domain-specific systems may assign moderate significance to each individual signal while overlooking their combined escalation trajectory [7]. Dynamic third-party intelligence therefore requires cross-domain models capable of detecting temporal co-occurrence, reinforcing deterioration, dependency concentration, and compound threats [13]. Addressing this analytical gap enables organizations to recognize when interacting weak signals collectively represent a materially greater threat to supply continuity.

3. MULTI-DOMAIN DATA ARCHITECTURE AND TEMPORAL SIGNAL ENGINEERING

3.1 Geopolitical and Geographic Exposure Signals

Geopolitical intelligence should convert broad international developments into supplier-specific indicators of potential disruption [13]. Relevant variables include sanctions designations, export restrictions, tariffs, political-instability measures, regional conflict intensity, trade-policy changes, port restrictions, and border disruption. Exposure should also capture dependence on strategic commodities whose production or processing is geographically concentrated [16]. Rather than assigning identical country-level risk to every supplier, the analytical architecture should map events to supplier facilities, upstream sources, transportation corridors, ports, and critical materials. Geographic concentration can be expressed as:

$$GC_i = \sum_{r=1}^R s_{i,r}^2$$

where $s_{i,r}$ represents the proportion of supplier i 's relevant activity concentrated in region r . Higher concentration can increase vulnerability when production and logistics dependencies coincide within an exposed geography [20].

3.2 Cybersecurity and Digital Dependency Signals

Cybersecurity monitoring should capture both observable security deterioration and the digital importance of each third-party relationship [14]. Predictive variables may include unresolved vulnerability findings, ransomware indicators, security incidents, authentication anomalies, patching delays, exposed internet-facing services, unusual privileged-access events, and repeated security-control failures. Cyber threat intelligence can supplement internal observations with information concerning active exploitation, malicious infrastructure, sector-targeted campaigns, and emerging vulnerabilities [18]. Digital dependency should additionally identify cloud platforms, APIs, managed services, software components, and remote-access relationships whose unavailability could interrupt supply-chain operations. A temporal cyber deterioration score may be represented as:

$$CD_{i,t} = \sum_{j=1}^m w_j x_{i,j,t}$$

where $x_{i,j,t}$ represents observed cyber-risk indicator j and w_j its analytical weight. Persistent deterioration is more informative than an isolated security exception, particularly when vulnerabilities coincide with critical digital dependencies [22].

3.3 Operational and Supply-Performance Signals

Operational data provide direct evidence of whether emerging external or internal pressures are beginning to affect supplier execution [15]. Relevant indicators include order-fulfilment ratios, promised-versus-actual delivery slippage, lead-time volatility, capacity utilization, production downtime, quality failures, order cancellations, shipment frequency, inventory availability, and logistics exceptions. Fulfilment performance can be represented as:

$$FR_{i,t} = \frac{Q_{i,t}^{delivered}}{Q_{i,t}^{ordered}}$$

Declining fulfilment combined with increasing delivery variability may indicate more significant deterioration than either signal independently [19]. Recurrent equipment outages, falling shipment frequency, or rising defect rates can similarly indicate weakening operational capability. These indicators should be assessed against supplier-specific historical behaviour because normal lead times, capacity patterns, and delivery variability differ substantially across suppliers, products, sectors, and transportation environments [21].

3.4 Commercial and Transactional Behaviour

Commercial behaviour can reveal changing supplier conditions before formal operational failure becomes visible. Procurement-volume changes, abrupt price increases, unusual payment requests, contract amendments, purchasing changes, and revised service commitments should therefore form part of dynamic monitoring [17]. Repeated requests to renegotiate delivery schedules or contractual conditions may become particularly informative when accompanied by worsening operational or external indicators. Communication deterioration—including delayed responses, repeated unresolved exceptions, or reduced reporting consistency—can provide additional behavioural evidence [20]. These variables should not automatically be interpreted as distress signals in isolation. Their predictive value arises from persistence, deviation from established supplier behaviour, and interaction with geopolitical, cybersecurity, financial, or operational deterioration occurring during the same analytical period.

3.5 Supplier Dependency and Network Exposure

Third-party risk severity depends not only on the probability of disruption but also on the supplier's structural importance within the supply network [13]. Dependency variables should capture single-source relationships, supplier criticality, tier-one and tier-two connections, alternative-source availability, geographic concentration, shared infrastructure, and recovery difficulty. Network representation can be formalized as:

$$G = (V, E)$$

where V represents suppliers, facilities, technologies, materials, and logistics nodes, while E captures their dependency relationships. Network centrality can identify third parties whose disruption may propagate across multiple products or facilities [18]. Substitutability should incorporate whether technically qualified alternatives exist, their available capacity, and the time required for activation. Shared ports, cloud providers, upstream manufacturers, or transportation corridors can also create hidden concentration [21]. Dependency intelligence therefore distinguishes isolated supplier vulnerability from exposure capable of producing cascading operational consequences.

3.6 Temporal Synchronization and Cross-Domain Feature Engineering

Multi-domain intelligence requires heterogeneous signals to be aligned according to when information actually became observable [14]. Rolling windows can capture recent averages and volatility, while lag variables identify delayed relationships between external events and supplier deterioration. Trend slopes, recurrence counts, persistence measures, and event-proximity variables provide additional temporal structure [16]. Supplier-specific standardized deviation can be expressed as:

$$Z_{i,t} = \frac{x_{i,t} - \mu_i^{base}}{\sigma_i^{base}}$$

Cross-domain features should capture interactions such as geopolitical escalation occurring simultaneously with logistics delays or heightened cyber activity [22]. Data from different reporting frequencies must be synchronized without retrospectively assigning later information to earlier prediction periods. Strict availability timestamps are therefore necessary to prevent information leakage and preserve realistic forecasting conditions [19].

Table 1. Multi-Domain Signal Architecture for Dynamic Third-Party Risk Intelligence

Risk Domain	Representative Signals	Temporal Feature	Update Frequency	Risk Interpretation	Operational Source
Geopolitical	Sanctions, conflict, export controls, tariffs, border restrictions	Event proximity; regional exposure trend	Daily/event-driven	Increasing exposure to political or trade disruption	Government, geopolitical and trade-risk feeds
Cybersecurity	Vulnerabilities, incidents, authentication anomalies, ransomware indicators	Recurrence; unresolved-risk duration; cyber deterioration score	Near-real-time/daily	Increasing probability of digital compromise or service interruption	SOC, SIEM, vulnerability and threat-intelligence systems
Operational	Fulfilment, capacity, downtime, defects, cancellations	Rolling deterioration; baseline deviation	Daily/weekly	Weakening supplier execution capability	ERP, QMS and supplier-performance systems
Commercial	Pricing, contracts, payment requests, communication exceptions	Behavioural change rate; persistence	Daily/weekly	Abnormal commercial behaviour or relationship deterioration	Procurement and contract-management systems
Logistics	Lead times, shipment frequency, port delays, transit exceptions	Lead-time volatility; repeated milestone failure	Near-real-time/daily	Increasing transportation and delivery instability	TMS, carrier and shipment-tracking feeds
External	Commodity prices	Volatility; event severity	Daily/event-	External pressure capable of	Market, infrastructure and

Risk Domain	Representative Signals	Temporal Feature	Update Frequency	Risk Interpretation	Operational Source
	infrastructure outages, weather, economic conditions	exposure duration	driven	amplifying supplier vulnerability	external-risk feeds
Dependency	Single sourcing, tier relationships, centrality, substitutability	Dependency concentration; recovery-time change	Monthly/event-driven	Potential for supplier disruption to propagate across the network	Procurement, supplier-mapping and continuity systems

4. DYNAMIC PREDICTIVE ANALYTICS AND CROSS-DOMAIN RISK INTELLIGENCE

4.1 Temporal Third-Party Risk Representation

Third-party risk should be modelled as an evolving trajectory because supplier vulnerability rarely emerges as a single observable event [21]. Geopolitical exposure, cyber weaknesses, delivery instability, and commercial deterioration may accumulate at different rates before collectively affecting continuity. Sequential observations preserve the ordering of these changes, while rolling windows distinguish temporary deviations from sustained deterioration [24]. For supplier i , temporal change can be represented as:

$$TD_{i,t}^{(w)} = \frac{1}{w} \sum_{k=0}^{w-1} (x_{i,t-k} - x_{i,t-k-1})$$

Persistence measures determine whether adverse conditions remain active, whereas acceleration captures increasing deterioration intensity [27]. Event sequences can additionally reveal whether one risk precedes another. Prediction horizons such as 7, 30, or 60 days enable risk trajectories to be translated into different intervention windows [30].

4.2 Machine-Learning Models for Dynamic Risk Prediction

Machine-learning models offer complementary capabilities for converting multidimensional supplier histories into disruption probabilities. Logistic regression provides a transparent baseline and allows directional interpretation of individual risk variables [22]. Random forests accommodate nonlinear relationships and interactions among geopolitical, cybersecurity, operational, and dependency indicators without imposing a predetermined functional structure [25]. Gradient boosting and XGBoost can progressively learn complex combinations of weak deterioration signals and are particularly useful for structured multi-source datasets [28]. Support vector machines can identify complex decision boundaries in high-dimensional feature spaces, whereas neural networks provide greater flexibility for modelling extensive sequential and nonlinear interactions [31]. Ensemble methods combine predictions from complementary models:

$$P_{i,t}^{ens} = \sum_{m=1}^M w_m P_{i,t}^{(m)}, \quad \sum_{m=1}^M w_m = 1$$

Model selection should consider calibration, temporal stability, interpretability, robustness across supplier categories, false-negative exposure, and warning lead time rather than classification accuracy alone [23].

4.3 Cross-Domain Anomaly and Compound-Threat Detection

Supervised prediction should be supplemented with anomaly detection because emerging third-party threats may differ from historically labelled disruptions [26]. Isolation-based methods, clustering, reconstruction-error models, and supplier-specific baseline analysis can identify unusual combinations of signals even when each individual indicator remains below a conventional escalation threshold. Compound risk can be represented conceptually as:

$$CR_{i,t} = f(G_{i,t}, C_{i,t}, O_{i,t}, I_{i,t})$$

where $G_{i,t}$ represents geopolitical exposure, $C_{i,t}$ cybersecurity risk, $O_{i,t}$ operational deterioration, and $I_{i,t}$ cross-domain interaction intensity. A moderate increase in regional instability may therefore become substantially more significant when accompanied by cyber threat escalation and deteriorating logistics performance [29]. Cross-domain anomaly detection identifies these reinforcing configurations rather than evaluating geopolitical, digital, and operational evidence independently [32]. Persistence and temporal proximity should further distinguish coincidental co-occurrence from an emerging compound threat.

4.4 Dynamic Third-Party Risk Score Construction

Predicted disruption probability should be converted into an operational score that reflects both likelihood and potential supply-network consequence [24]. A dynamic third-party risk score can be expressed as:

$$DTR_{i,t} = P_{i,t} \times C_i \times D_i \times R_{i,t}$$

where $P_{i,t}$ is predicted disruption probability, C_i supplier criticality, D_i dependency exposure, and $R_{i,t}$ represents persistence or deterioration intensity. The

dependency component should additionally reflect substitutability and recovery difficulty because identical disruption probabilities can produce very different consequences across suppliers [27]. For example, a moderately vulnerable single-source supplier with limited alternatives may require greater attention than a higher-risk supplier that can be replaced rapidly. Scores should be recalculated whenever material geopolitical events, cyber observations, operational changes, or dependency information become available [30]. The resulting trajectory indicates whether exposure is stabilizing, accelerating, or recovering rather than presenting risk as a static classification.

4.5 Explainable Cross-Domain Risk Attribution

Explainability is necessary because a composite score alone does not indicate why supplier exposure has changed. Global feature importance can identify the variables that consistently influence predictions across the supplier population, while local attribution methods can explain individual supplier classifications [23]. A local explanation can be represented as:

$$f(x_i) = \phi_0 + \sum_{j=1}^p \phi_{ij}$$

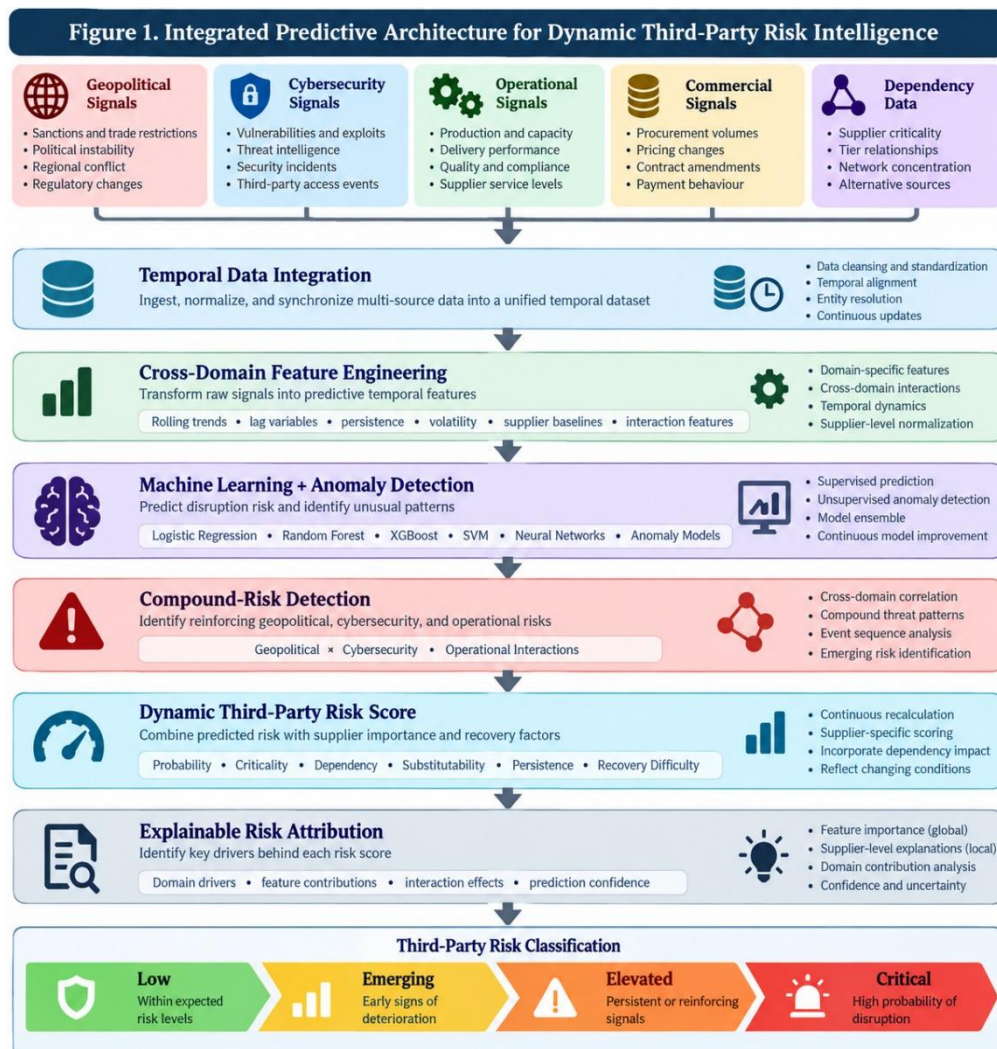
where ϕ_{ij} represents the contribution of feature j to supplier i 's predicted risk. Attribution may reveal that an elevated classification is driven primarily by sanctions exposure, unresolved cyber vulnerabilities, repeated delivery slippage, or interaction among several moderate indicators [26]. Explanations should separate domain-specific drivers from compound effects so that procurement, cybersecurity, operations, and enterprise-risk teams can validate the evidence and determine which function should lead intervention [31].

4.6 Dynamic Thresholds and Early-Warning Classification

Dynamic scores should be translated into differentiated warning states rather than a binary risk decision [22]. **Low** risk represents conditions within expected supplier baselines; **Emerging** identifies early deterioration requiring closer observation; **Elevated** reflects persistent or reinforcing signals requiring cross-functional review; and **Critical** indicates substantial exposure requiring urgent resilience action [28]. Classification can be expressed as:

$$State_{i,t} = g(DT, R_{i,t}, CR_{i,t}, PERS_{i,t}, CONF_{i,t})$$

where $PERS$ measures persistence and $CONF$ prediction confidence. Escalation thresholds should incorporate supplier criticality so that strategically important dependencies receive appropriately earlier review [32]. Persistence requirements can prevent temporary anomalies from producing unnecessary interventions, while confidence-aware classification directs uncertain predictions toward enhanced monitoring. Risk states should also permit de-escalation when adverse indicators reverse and sustained evidence demonstrates supplier recovery [25].



5. RISK PRIORITIZATION AND PROACTIVE RESILIENCE INTERVENTION

5.1 Translating Dynamic Risk Intelligence Into Coordinated Decisions

Dynamic third-party risk intelligence becomes valuable when it creates a shared basis for coordinated action across organizational functions [30]. Procurement teams can interpret supplier criticality and commercial exposure, while cybersecurity functions evaluate digital vulnerabilities, privileged access, and threat activity. Operations and logistics teams determine potential effects on production, transportation, inventory, and fulfilment [33]. Enterprise-risk and business-continuity functions can then assess whether combined exposure threatens broader organizational objectives or critical services. Rather than allowing each function to escalate independently, the framework should associate risk states with predefined cross-functional response protocols [36]. An elevated score driven primarily by cybersecurity indicators may require security-led investigation, whereas simultaneous geopolitical, logistics, and dependency deterioration may demand enterprise-level escalation [39]. Shared explanations, prediction confidence, and deterioration persistence therefore support proportionate intervention and clearly assigned decision ownership.

5.2 Geopolitical Exposure Mitigation

Geopolitical mitigation should reduce dependence on locations, resources, and transportation pathways vulnerable to political or trade disruption [31]. Geographic diversification can distribute sourcing across jurisdictions, while alternative trade routes reduce reliance on exposed ports, borders, or transit corridors. Where supplier relocation is commercially feasible, organizations can evaluate production alternatives in less concentrated regions [34]. Sanctions screening should be continuously updated to identify changing restrictions affecting suppliers, beneficial owners, materials, or counterparties. Strategic inventory can provide temporary protection where geopolitical deterioration threatens critical inputs [37]. Alternative material sourcing and prequalified regional suppliers further improve flexibility. Contingency planning should therefore connect geopolitical warning indicators with specific sourcing, transportation, inventory, and contractual responses rather than treating geopolitical intelligence solely as contextual information.

5.3 Cybersecurity Intervention and Digital Containment

Cybersecurity escalation should reflect both observed threat deterioration and the operational significance of the affected digital relationship [32]. Elevated cyber risk can trigger enhanced monitoring, credential reviews, vulnerability remediation, and reassessment of third-party access privileges. Where compromise is suspected, temporary access restriction or network segmentation can limit propagation while investigation proceeds [35]. API connections, remote administration channels, cloud integrations, and privileged accounts should receive particular attention where they provide pathways into critical systems. Incident coordination arrangements should define how suppliers exchange indicators, containment information, and recovery status during an active event [38]. For highly dependent digital services, organizations should evaluate alternative technology providers, backup communication mechanisms, data-recovery capability, and manual operating procedures. These controls convert cyber-risk intelligence into containment measures while preserving essential operational continuity where possible [40].

5.4 Operational Continuity and Alternative Sourcing

Operational deterioration requires interventions aligned with both warning horizon and available recovery time. Where predicted disruption exceeds acceptable exposure, organizations may increase safety stock, accelerate planned purchases, reserve production capacity, or redistribute inventory between facilities [30]. Dual sourcing can reduce concentration, although alternative suppliers should be technically qualified before an emergency where feasible [34]. Rapidly escalating risk may justify emergency procurement, production resequencing, or prioritization of products with limited substitute components. Logistics rerouting can bypass affected ports, carriers, or transportation corridors when disruption is geographically concentrated [37]. Mitigation intensity should also consider inventory coverage and alternative-source activation time. A high-risk supplier with sufficient stock protection may permit controlled intervention, whereas a moderately elevated single-source supplier supporting near-term production can require earlier action because response options diminish as inventory is consumed [39].

5.5 Dependency-Aware Prioritization and Cascading Failure Prevention

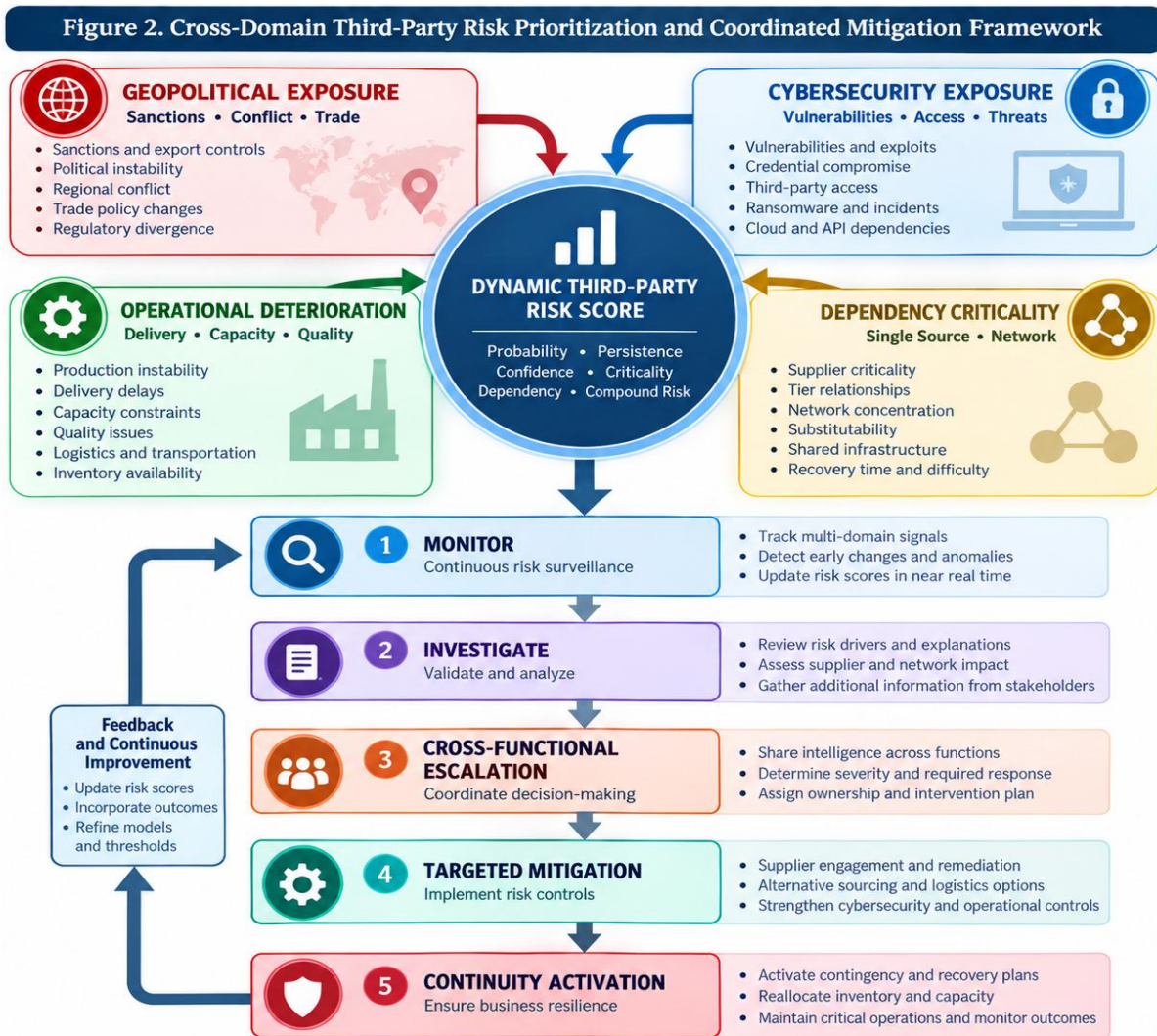
Risk probability alone does not adequately represent the potential consequences of third-party disruption. Dependency mapping should identify critical suppliers, common tier-two providers, shared technologies, geographic clusters, transportation corridors, cloud platforms, and infrastructure dependencies capable of creating correlated failures [33]. Propagation-sensitive prioritization can be expressed as:

$$PRI_{i,t} = DTR_{i,t} \times C_i \times NC_i \times (1 - S_i)$$

where $DTR_{i,t}$ represents dynamic third-party risk, C_i operational criticality, NC_i network concentration or centrality, and S_i substitutability. A moderately exposed supplier occupying a single point of failure may consequently warrant earlier intervention than a higher-risk supplier with several readily available substitutes [36]. Shared dependencies are particularly important because apparently independent suppliers may rely on the same upstream manufacturer, cloud platform, strategic commodity, or logistics route [38]. Prioritizing propagation potential enables organizations to direct limited resilience resources toward exposures capable of generating cascading disruption [40].

5.6 Closed-Loop Intervention and Adaptive Risk Intelligence

Each intervention should generate outcome data that strengthen subsequent risk prediction [31]. Recorded outcomes should distinguish events that materialized, intensified, stabilized, were contained, or were prevented following mitigation. A prediction should not automatically be labelled incorrect when timely intervention prevented the anticipated disruption [35]. Intervention records should therefore preserve the original warning, explanation, action taken, response timing, supplier outcome, and operational consequence. These observations can support threshold recalibration, feature refinement, model retraining, and improved estimation of intervention effectiveness [39]. Closed-loop learning consequently transforms risk management from repeated prediction into an adaptive process that learns which warnings and mitigation strategies provide the greatest resilience value.



6. PERFORMANCE EVALUATION, GOVERNANCE, AND RESPONSIBLE DEPLOYMENT

6.1 Temporal Experimental Design and Validation

Evaluation of dynamic third-party risk models should reproduce the chronological conditions under which real warnings would be generated [33]. Historical observations should therefore be divided into training, validation, and untouched testing periods rather than randomly mixed across time. Rolling or expanding-window validation can assess whether models remain reliable as geopolitical conditions, cyber threats, and supplier performance evolve [36]. All variables must be timestamped according to when information actually became available, preventing future sanctions, incident outcomes, or disruption records from leaking into earlier predictions [39]. Event-based testing should additionally examine performance around major cyber incidents, geopolitical shocks, and operational disruptions. Stratification across supplier sectors, geographic exposures, criticality levels, and disruption categories determines whether predictive reliability generalizes beyond dominant supplier groups [35].

6.2 Predictive and Early-Warning Performance

Performance evaluation should measure both statistical discrimination and whether warnings provide sufficient time for resilience action. Precision indicates the proportion of alerts corresponding to genuine disruption events, whereas recall measures the proportion of actual events successfully detected [34]. F1-score balances these measures, while ROC-AUC evaluates discrimination across classification thresholds. PR-AUC is particularly useful when major third-party disruptions are comparatively infrequent [37]. Specificity and false-positive rate quantify unnecessary alerts, whereas:

$$FNR = \frac{FN}{TP + FN}$$

captures missed disruptions that may leave organizations without adequate preparation [40]. Probability calibration should determine whether predicted risk levels correspond with observed event frequencies. Warning lead time should measure the interval between initial actionable detection and disruption, while actionable-warning rate evaluates how frequently predictions provide sufficient time to implement realistic mitigation [36].

6.3 Cross-Domain and Compound-Risk Evaluation

Integrated models should demonstrate whether combining domains provides information beyond independent risk monitoring. Evaluation should therefore compare geopolitical-only, cybersecurity-only, operational-only, and fully integrated architectures using identical chronological test periods [33]. Particular attention should be given to events where no individual domain exceeds its conventional warning threshold but several moderate indicators deteriorate concurrently [38]. Incremental predictive value can be assessed through changes in recall, PR-AUC, calibration, false-negative exposure, and warning lead time. Event-level analysis should additionally determine whether integrated models identify compound disruptions earlier than domain-specific alternatives [40]. This approach tests the central proposition that cross-domain interaction provides actionable intelligence unavailable from isolated risk indicators.

6.4 Benchmarking Against Conventional Third-Party Risk Assessment

Dynamic intelligence should also be benchmarked against the assessment mechanisms organizations would otherwise employ. Relevant comparators include periodic supplier questionnaires, static scorecards, scheduled cybersecurity assessments, geopolitical watchlists, operational thresholds, and manually consolidated enterprise-risk reviews [35]. Benchmarking should apply common disruption definitions and evaluation periods to avoid artificially favouring predictive approaches. Conventional methods may offer transparency and established governance but can lose sensitivity between assessment cycles [38]. Integrated predictive intelligence should therefore be evaluated according to earlier detection, cross-domain visibility, adaptation to changing conditions, false-negative reduction, scalability, and intervention usefulness rather than algorithmic complexity alone [34]. Comparative assessment establishes whether additional analytical sophistication produces measurable operational resilience value.

6.5 Governance, Privacy, Explainability, and Human Oversight

Integrated risk intelligence can contain commercially confidential supplier records, sensitive cybersecurity information, contractual data, and externally sourced threat intelligence, requiring clearly defined governance controls [37]. Data provenance should document origin, ownership, update frequency, transformation, and authorized use. Model drift and changing feature distributions require continuous monitoring because relationships learned under earlier geopolitical or cyber conditions may weaken over time [39]. Performance should also be evaluated across supplier sizes, sectors, regions, and data-availability levels to identify systematic bias. Explainable outputs should preserve the principal evidence underlying each escalation so that authorized personnel can validate predictions before consequential action [33]. Audit trails should record model versions, risk scores, explanations, overrides, decisions, and intervention outcomes. Human ownership of escalation and mitigation decisions remains essential for responsible deployment [40].

Table 2. Comparative Evaluation of Siloed and Integrated Third-Party Risk Intelligence

Evaluation Dimension	Siloed Assessment	Integrated Predictive Intelligence	Measurement Indicator	Resilience Benefit
Detection timing	Periodic or event-triggered review	Continuous temporal early warning	Median warning lead time	More preparation time before disruption
Cross-domain visibility	Risks evaluated separately	Geopolitical, cyber, operational and dependency signals jointly analysed	Compound-event detection rate	Identifies interacting threats
Adaptability	Predetermined review cycles and thresholds	Scores update as new signals emerge	Calibration/drift performance	Responds to changing conditions
Explainability	Domain-specific reports and expert judgement	Supplier-specific risk attribution across domains	Explanation fidelity and stability	Supports evidence-based escalation
False-negative exposure	Weak interacting signals may remain undetected	Cross-domain deterioration incorporated into prediction	False-negative rate	Reduces missed high-consequence threats
Scalability	Significant manual coordination	Automated monitoring across supplier populations	Suppliers monitored per assessment cycle	Extends continuous oversight

Evaluation Dimension	Siloed Assessment	Integrated Predictive Intelligence	Measurement Indicator	Resilience Benefit
Intervention utility	Actions frequently follow separate functional reviews	Shared risk score informs coordinated intervention	Actionable-warning rate	Supports earlier cross-functional mitigation

7. STRATEGIC IMPLICATIONS FOR UNITED STATES SUPPLY-CHAIN RESILIENCE

7.1 Enterprise Risk and Cross-Functional Integration

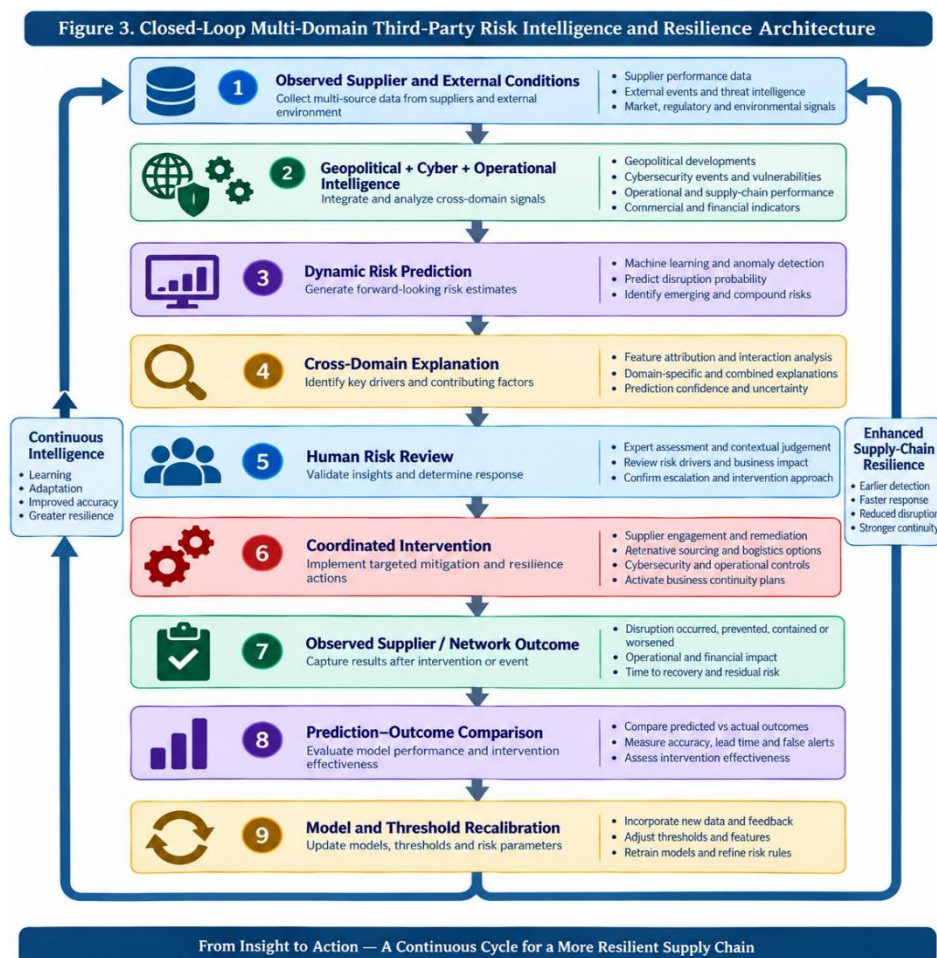
Dynamic third-party intelligence can provide a common analytical layer connecting procurement governance, cybersecurity operations, supplier management, enterprise risk, and business continuity [34]. Shared risk trajectories allow strategic sourcing teams to consider supplier vulnerability alongside cybersecurity exposure and operational dependency, while executives can prioritize resilience resources according to potential organizational consequences [37]. Integration therefore reduces fragmented escalation and enables procurement, security, operations, and continuity teams to coordinate interventions around a consistent representation of changing third-party exposure [40].

7.2 Critical Supply Networks and Systemic Resilience

Cross-domain intelligence has particular relevance where third-party failure can affect essential services or economically significant supply networks. Manufacturing organizations can monitor critical production dependencies, while healthcare and energy networks can identify suppliers whose disruption threatens essential equipment, materials, infrastructure, or services [35]. Transportation, financial services, telecommunications, and technology organizations similarly depend on interconnected physical and digital third parties [38]. Identifying common providers, geographic concentrations, technology dependencies, and shared logistics pathways can therefore support earlier recognition of vulnerabilities capable of producing systemic consequences [33].

7.3 Future Organizational and Analytical Direction

Future adoption requires interoperable supplier-intelligence ecosystems capable of combining multi-tier operational information with cyber, geopolitical, and dependency signals while maintaining appropriate security and confidentiality [36]. Responsible AI governance should accompany scalable real-time monitoring, with clear standards for explainability, auditability, model oversight, and human decision authority [39]. Secure cross-industry information sharing could further improve visibility of common dependencies and emerging threats that remain difficult for individual organizations to observe independently [40].



8. CONCLUSION

8.1 Synthesis of Principal Findings

This article demonstrates that third-party vulnerability is more effectively understood when geopolitical, cybersecurity, operational, commercial, and dependency signals are integrated within a unified analytical framework. Temporal synchronization enables changing supplier conditions to be evaluated as evolving trajectories rather than isolated observations. Combining these signals improves visibility of compound threats that may remain concealed within separate risk domains, enabling earlier identification of deteriorating conditions and providing organizations with greater opportunity to protect supply continuity before disruption becomes severe.

8.2 Analytical and Resilience Contribution

The framework advances third-party risk management from fragmented, periodic assessment toward dynamic, explainable, and dependency-aware intelligence. By connecting predictive risk scores and cross-domain explanations directly with coordinated intervention, it establishes a practical link between early-warning analytics and proactive organizational resilience.

8.3 Future Research Directions

Future research should investigate graph-based multi-tier modelling, cyber-geopolitical interactions, streaming threat intelligence, causal risk modelling, adaptive thresholds, and privacy-preserving data integration. Longitudinal studies should further determine whether predictive interventions produce sustained improvements in supply-chain resilience across different industries and disruption environments.

REFERENCE

1. Badea M, Bucoveţchi O, Gheorghe AV, Hnatiuc M, Raicu G. Maritime industry cybersecurity threats in 2025: Advanced persistent threats (APTs), hacktivism and vulnerabilities. *Logistics*. 2025 Dec 18;9(4):178.
2. Türkeş MC. How digitalization drives supply chain performance in the Romanian industry: The roles of sustainability, resilience, risk management, and integration. *Sustainability*. 2025 Nov 6;17(21):9895.
3. Okusi O, Chukwuani EN, Ikemefuna CD. Developing Real-Time Cyber Threat Intelligence Systems for Securing Algorithmic Trading, Digital Payments, and Financial Market Infrastructures. *Journal homepage: www.ijrpr.com ISSN*. 2025;2582:7421.
4. Chukwunweike J. Coordinating PLC-based load shedding and variable-speed drives to prevent transformer overloading during industrial production peaks. *Int J Electr Data Commun*. 2025;6(2 Pt B):118-135. doi:10.22271/27083969.2025.v6.i2b.109.
5. Nagesh A. Emerging financial risks-2025 & beyond. Available at SSRN 5241889. 2025 May 5.
6. Kumar S, Tripathi K, Das S. Cybersecurity of energy systems. In *Methods in Chemical Process Safety* 2025 Jan 1 (Vol. 9, pp. 297-339). Elsevier.
7. Obunadike TC. Leveraging AI forecasting to quantify tariff-induced food price volatility in net-importing nations. *Int J Res Publ Rev*. 2025;6(6):12441-12458. doi:10.55248/gengpi.6.0625.23102.
8. Healy N. "My way or the Huawei": Understanding the role of third-party states in weaponized interdependence via a study of the United Kingdom's response to the United States' treatment of Huawei. Available at SSRN 4540582. 2023 May 26.
9. Taheri Hosseinkhani N. Global food security amid geopolitical tensions and climate risk: Trade governance and adaptive strategies. Available at SSRN 5448314. 2025 Aug 14.
10. Samuel Addo. Harnessing AI-powered financial forecasting tools to improve risk management, investment strategies, and overall corporate profitability across industries. *International Journal of Science and Research Archive*, 2023, 09(02), 1175-1192. Article DOI: <https://doi.org/10.30574/ijrsra.2023.9.2.0653>
11. Avrahami Z, Zwillig M, Hajaj C. Leveraging OSINT for advanced proactive cybersecurity: Strategies and solutions. *IEEE Access*. 2025 Aug 28.
12. Skeete JP, Shaikh SA. Silicon safeguards: Open innovation as a shield against cyber risks. *Journal of Open Innovation: Technology, Market, and Complexity*. 2025 Sep 1;11(3):100628.
13. Ogan RK. Predictive anomaly detection for real-time virtual account transactions and API-driven payment processing across enterprise banking platforms. *Int J Comput Appl Technol Res*. 2024;13(12):298-308. doi:10.7753/IJCATR1312.1023.
14. Botschner J, Corley C, Fraser ED, Kotak R, McMahon D, Newman L. Cybersecurity in digital agriculture: a national security risk?. In *(In) Security: Identifying the Invisible Disruptors of Security* 2024 Oct 13 (pp. 281-315). Cham: Springer Nature Switzerland.
15. Culler MJ, Stolworthy RV, Heeter P, Tylecote A, Ponto T, Kmiec J, Martin L. Securing the modern grid: Federal investments, digitization, and supply chain strategy. Idaho National Laboratory Technical Report INL/RPT-25. 2025 Nov 1;89606.
16. Samuel Addo. Causal AI for strategic business planning: uncovering latent drivers of long-term organizational performance and resilience. *World Journal of Advanced Research and Reviews*, 2025, 26(2), 895-912. Article DOI: <https://doi.org/10.30574/wjarr.2025.26.2.1738>
17. George AS. Cyber resilience in an AI-driven world: A strategic framework. *Partners Universal Innovative Research Publication*. 2025 Dec 25;3(6):86-118.
18. Past LL. Preparing for the next disruption. *Supply chain disruptions and impact on global inflation*. 2025 Jun 6:253.
19. Ogan RK. Machine-learning framework for predicting point-of-sale integration failures across digital ordering, payment, and third-party delivery technology ecosystems. *Int J Res Publ Rev*. 2025;6(12):8887-8898.
20. Takeda M, Helms M, Watkins C. There is no chain without supply: strategic supply chain resilience through infrastructure initiatives and global SDGs. *Oper. Supply Chain Manage. Int. J.* 2024 Dec 16;17(4):384-401.
21. Racheal Kikachukwu Ogan. (2023). AUTOMATED CONFIGURATION COMPLIANCE ANALYTICS FOR DETECTING OPERATIONAL

DRIFT AND PREVENTING SERVICE DEGRADATION ACROSS MULTI-LOCATION RESTAURANT TECHNOLOGY SYSTEMS. INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM), 07(12), 807–819. <https://doi.org/10.5281/zenodo.22267240>

22. Shahzad K, Bakhtawar A, Tariq H. Analysing the role of adaptive risk management in empowering digital supply chain resilience. In *Technological Innovations and Industry 5.0* 2025 Jan 1 (pp. 227-240). Elsevier.
23. Farrand B. The economy–security nexus: Risk, strategic autonomy and the regulation of the semiconductor supply chain. *European Journal of Risk Regulation*. 2025 Mar;16(1):279-93.
24. Ethel Esinam Atubrah. The green transition and environmental justice: Understanding unequal community impacts. *Int J Geogr Geol Environ* 2026;8(8):12-24. DOI: [10.22271/27067483.2026.v8.i8a.844](https://doi.org/10.22271/27067483.2026.v8.i8a.844)
25. Kinney AB. Leveraging Artificial Intelligence for Supply Chain Risk Management. Institute for Homeland Security; 2024.
26. Magajiaka J, Adesanmi B. Lifecycle cost and resilience performance evaluation of climate-resilient urban road infrastructure under climate risk scenarios. *International Journal of Current Research*. 2026;18(5):37242-37251.
27. Evans A, Singh A, Golbin A. *Navigating Supply Chain Cyber Risk: A Comprehensive Guide to Managing Third Party Cyber Risk*. Taylor & Francis; 2025 Apr 22.
28. Racheal Kikachukwu Ogan. Machine-learning-based API failure prediction and root-cause analytics for improving reliability of enterprise banking integration architectures at scale. *Int J Comput Artif Intell* 2021;2(2):142-153. DOI: [10.33545/27076571.2021.v2.i2a.378](https://doi.org/10.33545/27076571.2021.v2.i2a.378)
29. Almohaimed M, Albalwy F, Alharbi R, Alqarni A, Aljohani A. Developing a comprehensive cyber risk assessment framework for supply chains: insights into third-party vulnerabilities and security gaps. *Intell. Inf. Manage*. 2025;17(3):58-77.
30. Ogan RK. Risk-based API governance for predicting integration failures, security anomalies, and service degradation across hybrid enterprise application environments. *Int J Finance Manage Econ*. 2024;7(2):871-882. doi:10.33545/26179210.2024.v7.i2.946.
31. Kalejaiye AN. Federated learning in cybersecurity: Privacy-preserving collaborative models for threat intelligence across geopolitically sensitive organizational boundaries. *Int J Adv Res Publ Rev*. 2025;2(07):227-50.
32. Ethel Esinam Atubrah. CLIMATE ADAPTATION POLICY AND COMMUNITY RESILIENCE: CULTURAL IDENTITY, LIVELIHOODS, AND ENVIRONMENTAL DISPLACEMENT. *International Journal of Science and Research Archive*, 2026, 20(02), 356–370. Article DOI: <https://doi.org/10.30574/ijrsra.2026.20.2.1635>.
33. Kalejaiye AN. Federated learning in cybersecurity: Privacy-preserving collaborative models for threat intelligence across geopolitically sensitive organizational boundaries. *Int J Adv Res Publ Rev*. 2025;2(07):227-50.
34. Khalil D, Nguyen NN. Long-term Supply Chain Risks: Scenario Planning Meets Natural Language Processing. Signature. 2025 May 9.
35. MGBAJIACA, JOHNBOSCO. 2025. “Co-Designing Resilient Infrastructure: Participatory Approaches for Sustainable Implementation”. *Current Journal of Applied Science and Technology* 44 (8):11-17. <https://doi.org/10.9734/cjast/2025/v44i84586>.
36. Lyu M, Farooq J, Zhu Q. Mapping cyber threats in the 5G supply chain: Landscape, vulnerabilities, and risk management. *IEEE Network*. 2024 Aug 12;39(1):251-60.
37. RASSHYVALOV D, NURAKHOVA B, ALBOSHCHII O, REIKIN V, BOCHAROVA N. Supply chain risk management as an integrated strategy for ensuring stability. *Journal of Applied Economic Sciences*. 2025 Sep 1;20(3).
38. Sternhell A. A Trusted Global Data Supply Chain. In *Data, Security, and Trust in Smart Cities 2024* Jun 27 (pp. 3-31). Cham: Springer Nature Switzerland.
39. Goyal NK. Weaponizing misinformation and cyberattacks on supply chains. In *Mass media and impact of fake news on supply chains 2025* (pp. 177-210). IGI Global Scientific Publishing.
40. Atubrah EE. Environmental justice movements and environmental policy change: the role of community knowledge and place-based action. *Int J Res Publ Rev*. 2026;7(1):1169-1180. doi:10.55248/gengpi.07.0826.2444