International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(12s) 2026 pp. 196-207
https://doi.org/10.70917/ijcisim-2026-3885
Article

Geopolitical Risk Mitigation in Information Governance:An Evaluation Framework for Algorithmic Bias and Data Security in AI-DrivenGlobal Supply Chains.

Iqra Nissar[1], Shreesh Pathak[2], Yogesh Kumar Gupta[3]

[1]Amity University, Noida, India. Email:iqralone.il@gmail.com
[2]Amity University, Noida, India. Email:skpathak@amity.edu
[3]Motilal Nehru College,Delhi University India. Email:yogeshgupta@mln.du.ac.in
Corresponding Author: Iqra Nissar (iqralone.il@gmail.com)

Abstract: Artificial intelligence (AI) is increasingly considered a cornerstone of contemporary discourse concerning geopolitics and geoeconomics.The domain appears to be largely constrained by a teleological, zero-sum narrative that prioritizes the question of which state will secure AI supremacy in this great power competition.This perspective diverts attention from a more critical and empirically accessible phenomenon that is the increasing utilization of artificial intelligence, data analytics and machine learning as fundamental instruments for geopolitical risk mitigation, supply chain oversight and state-led regulatory enforcement within an increasingly fragmented and competitive global economic landscape. This paper reconceptualises AI-driven supply chain risk management systems not merely as operational tools, but as critical sites of algorithmic governance where technical properties such as bias detection mechanisms, data security protocols, and cross-jurisdictional information routing function as direct variables of state power. By integrating structural realism with power transition theory, this study moves beyond aggregate AI capability metrics to examine the systemic institutionalisation of these technologies. The study employs a multidimensional evaluation framework that positions algorithmic bias exposure, data security, structural dependency concentration, and regulatory fragmentation risk as fundamental determinants of geopolitical leverage,implicating how automated systems actively reshape the global distribution of risk, information, and strategic control.To conceptualize the structural friction inherent in global digital supply chains, this paper introduces the 'algorithmic sovereignty trilemma.' This construct demonstrates why technical optimisation, data sovereignty, and cross-bloc interoperability cannot be simultaneously maximised, effectively mapping the fundamental trade-offs states must navigate amidst technological decoupling. The framework is applied illustratively to the semiconductor and critical-minerals supply chains implicated in the ongoing US-China technological rivalry, and is situated against the European Union's AI Act, United States export-control practice, and China's data-security architecture. The paper argues that algorithmic supply chain governance is best understood not as a neutral optimisation problem but as a site where distributional power, sovereignty claims, and systemic risk are jointly produced.The paper concludes that by foregrounding the technical architecture of supply chain oversight, states can better anticipate how algorithmic dependencies amplify security dilemmas and harden geopolitical fissures .It suggests a recalibration of national policy toward the creation of resilient, audit-transparent oversight architectures that mitigate asymmetric vulnerabilities and prevent the weaponization of critical data-flow interdependencies. By integrating technological expertise with systemic structural analysis, the research underscores how the securitization of AI value chains inevitably promotes the emergence of techno-blocs, which utilize exclusive infrastructure partnerships to consolidate authority over global digital inputs.

Keywords: Algorithmic governance,Supply chain risk management,Algorithmic bias,Structural realism,Technological decoupling

1. Introduction

In the emerging world order,Artificial Intelligence has transcended its status as a technological utility to become a structural pillar of geopolitical power, effectively serving as a primary instrument for negotiating national sovereignty and security in a multipolar landscape(Truby et al., 2026).It functions as both a foundational general-purpose technology, characterized by multi-sectoral diffusion permeating domains such as healthcare, defense, governance, and finance and has become the primary theater for systemic rivalry that acts as a primary catalyst for the consolidation of exclusionary digital ecosystems and the subsequent hardening of techno-nationalist barriers that fundamentally restructure the international digital order.This integration extends beyond domestic socio-economic shifts, forcing states to recalibrate their foreign strategies, restructure military-civil

innovation systems, and address the new dependencies that are reshaping global influence (Oludayo, 2024).So,in the contemporary era, artificial intelligence has emerged as a critical focal point of national survival, compelling superpowers to instrumentalize technological interdependence to safeguard strategic autonomy and fortify national security(Hendrycks et al., 2025; Schmidt, 2022)

The prevailing policy and scholarly literature on artificial intelligence and international politics remains persistently anchored in a reductionist, zero-sum vocabulary fixated on the question of who wins the AI race.This is supported by recent scholarly efforts that characterize the digital economy as an arena for elite-centered state intervention, where actors bypass multilateral oversight to assert control over key infrastructure through the creation of closed-loop techno-blocs (Weymouth, 2025). The escalating competition between the United States and China over AI is an example of this bifurcation, where the weaponization of interdependence and the pursuit of strategic autonomy compel middle powers to navigate a landscape defined by dual-use risks and the erosion of traditional civilian-military boundaries (Tran, 2026). It is seen as a not just a technological race but a fundamental contest for global leadership and the shaping of future international norms and structures .This competition has transformed into a multidimensional struggle that permeates military, economic, and trade sectors, reflecting a broader structural expression of great power rivalry in an anarchic global environment.It has prompted a profound re-evaluation of established international security frameworks, as both states navigate the dilemma of balancing technological integration with the risks of strategic vulnerability (Ilyinsky, 2026).

This perspective diverts attention from a more critical and empirically accessible phenomenon that is the increasing utilization of artificial intelligence, data analytics and machine learning as fundamental instruments for geopolitical risk mitigation, supply chain oversight and state-led regulatory enforcement within an increasingly fragmented and competitive global economic landscape.States are increasingly deploying algorithmic frameworks to codify regulatory norms and influence international standards, effectively projecting domestic governance models as global templates for digital authority (de-la-Morena, 2025). This shift towards digital standard-setting allows dominant powers to weaponize technical specifications and interoperability requirements, thereby institutionalizing their economic preferences within the very architecture of global digital commerce (Srivastava & Bullock, 2024).

This shift signifies a transition where sovereign authority is no longer strictly bound to territorial limits but is increasingly projected through the strategic manipulation of algorithmic governance mechanisms and the institutionalization of technical standards that define digital authority(Roberts et al., 2021). This evolution reflects a broader trend where technology acts as a medium of statecraft, enabling nations to reconstruct security and sovereignty by embedding their geopolitical interests into the foundational infrastructure of global networks (Hu et al., 2025). Consequently, the convergence of security and industrial strategy has incentivized the development of autonomous systems and semiconductor supply chains that function as critical nodes of strategic influence (Nikolić et al., 2025).

This paper reconceptualises AI-driven supply chain risk management systems not merely as operational tools, but as critical sites of algorithmic governance where technical properties such as bias detection mechanisms, data security protocols, and cross-jurisdictional information routing function as direct variables of state power. By examining how these systems automate the prioritization of certain trade flows over others, this analysis reveals how algorithmic decision-making actively shapes the geopolitical boundaries of economic interdependence (Almakaty, 2026). The deployment of advanced machine learning models allows for the preemptive mapping of complex supply chain dependencies, thereby enabling states to identify critical chokepoints in semiconductor and telecommunications sectors with unprecedented predictive accuracy(Stanojević, 2025). This capability facilitates the implementation of targeted export controls and foreign investment restrictions, effectively transforming latent economic interdependencies into active instruments of state-led regulatory enforcement (Vujičić, 2024).

The strategic calibration of enforcement measures underscores a transition away from maximalist sanctions toward nuanced regimes that seek to safeguard technological parity without inducing catastrophic supply chain fragmentation (Yoon et al., 2026). This granular approach reflects the broader shift toward digital federalism, where states leverage multi-tiered sovereignty to balance the necessity of global technological collaboration with the imperative to secure domestic strategic chokepoints (Ishkhanyan, 2025),(Beaumier & Cartwright, 2023). By integrating these predictive models, policymakers can now quantify asymmetric vulnerabilities with higher precision than traditional analytical frameworks, allowing for the preemptive securing of advanced node production sites (Rao, 2024). This methodology moves beyond simple reactive policy, facilitating a proactive recalibration of economic networks that acknowledges the distinct centralities held by states in design, raw material, and manufacturing equipment domains (Beaumier & Cartwright, 2023).

This framing, while politically resonant, appears to possess two structural weaknesses. First, the literature tends to treat artificial intelligence capability as a unitary, quasi-military asset whose accumulation appears to

determine relative power, in a manner analogous to dreadnought counts prior to 1914. Second, it diverts attention from the sites where AI is actually being institutionalised into the operating logic of states and firms: not in headline-grabbing frontier models, but in the mundane, distributed infrastructure of global risk management — credit scoring, customs screening, supplier vetting, and, centrally, supply chain risk management (SCRM). These mundane automated systems create essential bottlenecks in compute provision and chip manufacturing, where the concentration of technical authority allows states to institutionalize oversight and enforcement far more effectively than through high-level policy declarations (Muldoon et al., 2025). Such systems represent a departure from market-led innovation toward a model of state-industrial coordination, where the deliberate fusion of economic and security agendas facilitates the militarization of underlying foundational architectures (Amenitsky & Vorobyov, 2025). In this context, the integration of "military-civil fusion" programs further obscures the distinction between commercial enterprise and defense imperatives, compelling rival powers to implement increasingly restrictive measures to protect their technological sovereignty (Kilian, 2024).

The paper resolves to answer two critical questions:first, how do algorithmic risk management architectures enable states to codify and project their specific definitions of security into global supply chains; and second, to what extent does the reliance on singular "chokepoint economies" for advanced semiconductor fabrication force a decoupling of commercial and strategic imperatives. To address these inquiries, this analysis examines the vulnerability inherent in an inverted supply chain triangle, where the concentration of semiconductor fabrication in a single jurisdiction necessitates a delicate navigation of competing geopolitical pressures (Davies et al., 2024; Liu & Lin, 2025).

This inquiry facilitates a strategic shift in the analytical focus accordingly. Rather than asking which great power possesses superior AI, it asks how AI-driven systems structurally reshape the distribution of risk, information, and control within global supply chains, and how this reshaping interacts with state regulatory frameworks amid accelerating US-China technological decoupling. AI-driven supply chain risk management (AI-SCRM) systems appear to perform functions that were previously the preserve of sovereign authority: they classify counterparties as trustworthy or suspect, they determine which nodes of a production network are "critical" and therefore subject to onshoring or friend-shoring, and they mediate cross-border data flows that are themselves objects of national-security regulation. In this sense, AI-SCRM systems function not merely as neutral corporate risk-management tools, but as critical nodes of algorithmic governance. By formalizing classificatory criteria for 'trustworthiness' and 'security' within automated workflows, these systems effectively delegate enforcement authority to private actors, allowing states to project power and institutionalize oversight far more effectively than through traditional bureaucratic or legal instruments alone. This transition signifies a broader shift in statecraft, where technical parameters—such as supplier vetting and data-routing protocols—are transformed into direct variables of geopolitical power, effectively blurring the lines between commercial compliance and national strategic alignment.

The central contribution of this paper arguably comprises a structured evaluation framework that treats algorithmic bias and data security not as narrow technical compliance issues, but as variables with structural, geopolitical significance. The framework appears intended for utility in two registers simultaneously: as an analytical device for International Relations (IR) scholarship regarding the diffusion of algorithmic authority under great-power competition, and as a practical diagnostic that firms, regulators, and multilateral bodies may apply to specific Artificial Intelligence Supply Chain Risk Management (AI-SCRM) deployments. Section 2 outlines the conceptual method used to construct the framework and situates it within the relevant literatures. Section 3 presents the results: the theoretical construct of the algorithmic sovereignty trilemma, the four-dimensional evaluation framework, its illustrative application to the semiconductor and critical-minerals supply chain, and its positioning against current regulatory regimes. Section 4 discusses implications and limitations, and Section 5 concludes.

2. Materials and Methods

This study employs a multi-methodological approach to map the intersection of state-corporate power dynamics and algorithmic governance. Specifically, it utilizes a comparative governance analysis to evaluate how state-driven regulatory models and corporate-led AI implementations collide within global supply chains.The research integrates qualitative data from existing literature and expert reports to synthesize the ethical, legal, and technical complexities inherent in these governance structures. Furthermore, this analysis applies a bidirectional framework to categorize the fluid interactions between sovereign states and AI development firms, moving beyond the zero-sum interpretations that currently dominate discussions of technological competition(Abiri, 2025). This analytical lens facilitates a more granular examination of how power is both enhanced and eroded across political, economic, and technical domains .This study is primarily conceptual and theory-building, prioritizing the structural articulation of algorithmic governance over empirical statistical validation. Its methodology adheres to the rigorous standards of qualitative, literature-grounded framework construction

characteristic of International Relations and policy-analytic scholarship, providing a systematic lens to analyze the evolving intersection of state-corporate power dynamics and algorithmic technical oversight. To operationalize this theoretical construct, the methodology further incorporates an exploratory scenario modeling technique derived from General Morphological Analysis. This approach structures the complex, non-quantifiable relationships inherent in high-level AI oversight by mapping alternative future trajectories of power and institutional control..

2.1 Literature Review

The large group of scholars have extensively documented the proliferation of artificial intelligence as a cornerstone of national security and economic vitality among major powers and emphasized its role in influencing global power. Building upon this, current academic discourse increasingly highlights how states leverage these technologies to redefine public responsibility and institutional control within rapidly evolving regulatory regimes (Djeffal et al., 2022). However, this body of research often overlooks the mechanisms through which private sector AI deployment inadvertently subsumes traditional sovereign functions, creating gaps in existing governance models (Birkstedt et al., 2023). This literature review synthesis follows a systematic approach to identifying critical knowledge gaps within the current scholarly discourse surrounding governance regimes and technological authority . This process prioritizes an interdisciplinary integration of legal frameworks, policy evaluation, and theoretical perspectives to better describe the current state of fragmented AI governance . By synthesizing diverse strands of inquiry, this review characterizes how nascent regulatory mechanisms and institutional actors currently interact within a global landscape defined by competitive, non-linear trajectories (Schmitt, 2021). This systematic mapping reveals how existing scholarly efforts often address fragmented domains in isolation rather than capturing the systemic interdependence between security mandates and technical implementation . The initial phase integrated four rarely combined bodies of scholarship: technical and operations management regarding AI-driven supply chain risk; computer science and law concerning algorithmic bias in automated classification; political economy addressing data sovereignty and surveillance infrastructure; and International Relations theory on structural power and technological competition. This integrative approach enables the identification of critical knowledge gaps in the current scholarly discourse, facilitating a comprehensive understanding of the mechanisms through which regulatory adaptations emerge and stabilize across disparate governance regimes (Navarro-Meneses & Pablo-Martí, 2025). Subsequently, this synthesis serves to align fragmented disciplinary insights, fostering a cohesive theoretical framework that bridges the divide between abstract security objectives and concrete algorithmic constraints (Undheim, 2024). The triangulation of literature allows for the conceptualization of control-by-design principles, which translate high-level security mandates into verifiable architectural requirements (Nwachukwu et al., 2025). This systematic review ensures that the resultant framework is not merely speculative but grounded in established academic methodologies for analyzing transparency, accountability, and multi-stakeholder governance (Batool et al., 2025).

Each body of literature was scrutinized for its conceptualization of two primary analytical variables classificatory bias and data-jurisdictional exposure and for whether these variables may function as mere technical parameters or as structurally consequential determinants for the distribution of international power. By operationalizing these variables, this phase moves beyond characterizing AI merely as a technical enhancement, instead identifying how institutional and societal constraints actively reshape governance outcomes (Paul, 2023). This analytical decomposition elucidates the acute tension between normative governance objectives and the technical exigencies of systemic AI integration, illustrating how institutional design often fails to synchronize with the velocity of technological transformation, thereby creating an "oversight gap" that compromises regulatory efficacy(Reuel et al., 2024). This structural mismatch necessitates an evaluation of institutional capacity to respond to autonomous systems, addressing the conceptual vacuum that currently hinders the maturation of agentic accountability models (LEE, 2025). Building upon this, the study further examines how integrating cross-sectoral principles can bridge the disconnect between rigid legal standards and the rapid, iterative nature of algorithmic deployment (Robles & Mallinson, 2025). This interdisciplinary mapping reveals how technical safety standards and corporate governance protocols are increasingly co-opted to serve as instruments of geopolitical alignment. By identifying these thematic intersections, the analysis exposes a significant conceptual gap where contemporary regulatory discussions often fail to reconcile private technical standards with the exigencies of national security (Ness et al., 2024). Consequently, these normative tradeoffs necessitate a rigorous reassessment of how transparency and accountability mechanisms are calibrated to mitigate systemic risks within the AI lifecycle .The assessment incorporates human rights-based perspectives to ensure that accountability mechanisms extend beyond voluntary corporate self-regulation to encompass binding obligations for all private actors in the development pipeline.

2.2 Theoretical Framework

This section adopts a tri-lens paradigm to interrogate the mechanisms, societal impacts, and institutional adaptation requirements inherent in AI governance.By integrating structural realism with power transition theory, this study moves beyond aggregate AI capability metrics to examine the systemic institutionalisation of these technologies. This approach facilitates an analysis of how diverse jurisdictions prioritize conflicting institutional logics ranging from legal-bureaucratic certification to market-oriented innovation thereby fostering a fragmented global architecture characterized by divergent semantic architectures that render regulatory frameworks mutually unintelligible (Guo & Zhang, 2026). Structural realism provides a lens for understanding how states leverage AI to enhance sovereign security and competitive advantage, viewing technological dominance as a key determinant of the international distribution of power (Ge, 2025). It establishes a foundational basis for evaluating how sovereign interests incentivize the adoption of divergent, protective regulatory models that prioritize national control over transnational interoperability . Concurrently, power transition theory highlights how the rapid diffusion of these capabilities disrupts established hierarchies, compelling states to enact internal institutional adaptations to mitigate the externalities generated by such general-purpose technologies. It underscores how the resultant normative divergence complicates the establishment of unified governance frameworks, as states struggle to reconcile domestic security imperatives with the necessity of cross-border coordination .A new perspective , centered on regime-complex theory, offers a mechanism to map these overlapping institutional arrangements and identifies how non-state actors influence the formation of ad hoc normative clusters .Subsequent integration of these theoretical frameworks utilized structural realism and power transition theory as the primary analytical lens, positing that any technology that redistributes capabilityor is perceived to do so at an accelerating velocity may generate competitive dynamics irrespective of the intentions of the technology's designers. Such instability is further compounded by the emergence of multiplex governance, where a pluralist array of actors and regions weakens traditional hegemonic influence through fragmented, overlapping institutional initiatives . These decentralized clusters not only challenge monolithic global governance models but also illustrate the inherent difficulties in achieving international consensus when regimes remain intentionally narrow in scope.

This synthesis facilitated the development of the central conceptual construct: the algorithmic sovereignty trilemma. Extending Ishkhanyan's sovereignty internationalism paradox which posits that autonomous digital development inherently conflicts with the requirements of integrated global governance the trilemma formalizes these pressures as a set of structural, mutually exclusive constraints. (Ishkhanyan, 2025).By framing these tensions as a fundamental tri-directional conflict rather than mere policy oversight, this construct provides a robust analytical framework for diagnosing why contemporary regulatory attempts to reconcile national security with technological interoperability frequently falter.It captures the inherent tension between maintaining domestic regulatory autonomy, fostering international digital interoperability, and ensuring the economic competitiveness of domestic firms within a globalized AI market. Each vertex of this trilemma compels policymakers to sacrifice one objective in favor of another, as current attempts to achieve simultaneous optimization invariably lead to institutional instability and the fragmentation of global norm-setting processes.

In Section 3.1, which suggests that algorithmic bias and data security function as structurally linked trade-offs, rather than independent design choices. This dependency necessitates a shift from siloed technical mitigation to comprehensive regime-complex approaches that address the instability inherent in overlapping institutional jurisdictions . Adopting this perspective reveals that regime complexity often results in a patchwork of agreements that struggle to address the convergence of frontier sciences, thereby creating regulatory voids.This study's main theoretical basis rests upon the premise that systemic competition dictates the trajectory of institutional design, pushing states to prioritize security-focused, preemptive measures over collaborative, harmonized frameworks. Consequently, the pursuit of technological autonomy frequently exacerbates the sovereignty gap, as state legitimacy becomes increasingly contingent upon the domestic enforcement of restrictive, state-centric regulatory norms.

2.3 Framework Derivation and Indicator Selection

The third phase of the analysis operationalizes the trilemma into a four-dimensional evaluation framework. To ensure the model remains both theoretically rigorous and practically actionable, indicator selection adhered to two core criteria: first, grounding in established methodologies from the algorithmic-fairness, data-governance, or industrial-organisation literatures, ensuring the framework remains tractable for practitioners; and second, the plausible availability of metrics from data already collected for internal risk-management or regulatory-compliance purposes.To evaluate the framework's utility in capturing structural institutional friction, we applied it in an illustrative capacity while noting the lack of statistical validation to the semiconductor and critical-minerals supply chains. These sectors serve as ideal test cases, as they represent the nexus of globalized production and intense regulatory competition. The analysis utilized publicly available regulatory documentation from the European Union, the United States Bureau of Industry and Security, and secondary reporting on China's data-security regime, current as of mid-2026. Rather than seeking to function as a formal hypothesis test, this illustrative application serves as a necessary proof-of-concept, establishing the analytical utility of the

framework’s constructs within the paper's conceptual, non-empirical scope; potential limitations associated with this methodological choice are explicitly addressed in this paper.

3. Results

3.1 The Algorithmic Sovereignty Trilemma

The synthesis of structural realist principles and regime-complex theory yields a core proposition: states and firms operating within artificial intelligence-driven supply chains confront a rigid algorithmic sovereignty trilemma. Rather than a mere policy challenge, this trilemma represents a fundamental structural constraint where the simultaneous attainment of technical optimization, data sovereignty, and interoperability remains mathematically and politically untenable. Policymakers are thus compelled to prioritize one vertex, often sacrificing interoperability for the sake of enforcing restrictive, state-centric norms to mitigate the risks of foreign influence . This strategic shift underscores a transition toward "algorithmic imperialism," wherein advanced economies utilize AI as a mechanism to assert control over strategic resources and dictate global trade standards .In this environment, stakeholders are constrained to prioritize only two of the three objectives—technical optimisation, data sovereignty, and global interoperability as the simultaneous attainment of all three remains structurally infeasible. This trade-off implies that the European Union’s pursuit of jurisdictional independence, while intended to bolster strategic autonomy, often forces a withdrawal from broader, collaborative global standards in favor of localized, restrictive enforcement (Mügge, 2024). This trajectory reveals that EU AI policy consistently prioritizes jurisdictional independence over citizens' rights, ultimately reinforcing a competitive logic that prioritizes systemic power over harmonized international governance The simultaneous pursuit of all three appears structurally difficult: maximal technical optimisation favours the largest possible pooled dataset, which is precisely what data-sovereignty regimes such as China’s data-security law or the European Union’s data-localisation provisions are designed to constrain(Fu et al., 2020) and pursuing strict sovereignty compliance across multiple, mutually inconsistent jurisdictions degrades interoperability, forcing firms toward parallel, non-communicating system architectures ,a phenomenon that appears manifest in the bifurcation of cloud, chip, and model ecosystems between the United States and China(Klingler-Vidra, 2019).

This trilemma reframes algorithmic bias and data security as downstream expressions of a prior, structural choice regarding the prioritization of the trilemma’s dimensions. A system optimized for technical efficiency and interoperability may mitigate algorithmic bias by leveraging a more expansive, cross-border training dataset that captures a broader distribution of the supplier population,an outcome consistent with the established link between dataset representativeness and the mitigation of disparate-impact mechanisms in algorithmic-fairness literature., but higher structural data-security exposure, because that data crosses more jurisdictional boundaries. Conversely, a system that prioritises data sovereignty and interoperability within a single bloc will tend to exhibit lower cross-border security exposure but higher algorithmic bias, because its training data is drawn from a narrower and more homogeneous supplier population. The trilemma thus necessitates a structural trade-off, precluding simple technical remediation. This aligns with structural realist theory, which posits that positional power—determined by an actor’s location within the network rather than the intrinsic capability of its models—governs strategic advantage amidst the pressures of accelerating decoupling. Consequently, this institutional bifurcation accelerates the consolidation of power among digital platform firms that can navigate these fragmented regulatory landscapes, thereby entrenching global inequalities in the distribution of essential AI-enabling resources .

3.2 A Four-Dimensional Evaluation Framework

Extending the implications of the algorithmic sovereignty trilemma, we propose a four-dimensional evaluation framework for AI-driven supply chain risk management systems, summarized in Table 1. This framework operationalizes each dimension through discrete, observable indicators metrics predicated on existing organizational data streams typically harvested for internal risk governance and regulatory compliance—thereby ensuring both practical feasibility and methodological coherence. This framework incorporates elements of data stewardship and policy-as-code to move beyond mere compliance, enabling firms to audit decisioning stacks against shifting jurisdictional requirements.

Table 1. Four-Dimensional Evaluation Framework for Artificial Intelligence-Enabled Social Customer Relationship Management (AI-SCRM) Systems

Dimension	**Core Question**	**Representative Indicators**	**Governance Referent**	

Cross-border data flow mapping; encryption and access control maturity; third-party/vendor exposure; breach history	Cross-border data flow mapping; encryption and access control maturity; third-party/vendor exposure; breach history	A firm-level audit by a sectoral regulator.	A firm-level audit by a sectoral regulator.	
Cross-border data flow mapping; encryption and access control maturity; third-party/vendor exposure; breach history	Cross-border data flow mapping; encryption and access control maturity; third-party/vendor exposure; breach history	Cross-border data flow mapping; encryption and access control maturity; third-party/vendor exposure; breach history	National data-protection authority; export-control regime	
Cross-border data flow mapping; encryption and access control maturity; third-party/vendor exposure; breach history	Cross-border data flow mapping; encryption and access control maturity; third-party/vendor exposure; breach history	Cross-border data flow mapping; encryption and access control maturity; third-party/vendor exposure; breach history	Interstate; alliance-level coordination	
Regulatory Fragmentation Risk (RFR)	To what extent could the system be subject to a multiplicity of divergent compliance regimes, necessitating simultaneous adherence?		Count of overlapping AI/data statutes; conflict-of-law incidents; compliance lead time	Multilateral/plurilateral standard-setting bodies

Algorithmic Bias Exposure (ABE) may elucidate whether a system's risk classifications are systematically skewed against particular categories of supplier — by firm size, geographic origin, or digital-infrastructure maturity — independent of underlying commercial risk. Operationally, this necessitates the granular disaggregation of model error rates across disparate supplier cohorts, coupled with a mandatory audit verifying whether explainability outputs remain actionable for affected entities. This oversight is particularly critical for small and medium enterprises in the Global South, where the capacity to contest adverse algorithmic determinations is frequently constrained by systemic resource deficits and institutional barriers (Niikondo & Ziezo, 2026).

Data Security and Provenance elucidates the jurisdictional geography of the data pipeline: mapping where data is ingested, processed, and archived, and identifying which sovereign legal regimes possess the authority to compel disclosure or mandate data localization. By tracing these flows, the framework identifies whether the underlying infrastructure renders the firm vulnerable to foreign legal assertions or sudden shifts in data sovereignty requirements. This dimension treats data-flow mapping as equivalent to critical-infrastructure mapping in traditional security studies.

SStructural Dependency Concentration adapts the standard industrial-organization metric, the Herfindahl-Hirschman Index, to quantify the systemic reliance of AI-SCRM architectures on upstream inputs—specifically advanced semiconductors, cloud compute, frontier foundation models, and specialized human capital. By evaluating the geographic and institutional diversity of these supply chains, SDC offers a rigorous diagnostic for identifying latent vulnerabilities. High concentration in inputs sourced from a single state, particularly one characterized as a strategic competitor, transforms ostensibly benign commercial dependencies into potent geopolitical leverage; this dynamic is consistent with the "chokepoint" logic of weaponized interdependence developed by Farrell and Newman.

Regulatory Fragmentation Risk quantifies the compliance burden and legal-conflict risk inherent in navigating disparate, non-harmonized AI and data-governance regimes simultaneously. Crucially, the four dimensions are not aggregated into a single composite score, as such reductionism would obscure the strategic trade-offs inherent in the algorithmic sovereignty trilemma. Instead, the framework functions as a diagnostic profile: ABE and DSP reveal internal system vulnerabilities—specifically, which leg of the trilemma the system has deprioritized—while SDC and RFR delineate exposure to systemic, externally imposed shocks.

3.3 Illustrative Application: Semiconductor and Critical-Minerals Supply Chains

The framework can be illustrated, though not yet fully operationalised in the absence of proprietary firm-level data, using the semiconductor and critical-minerals supply chains at the centre of contemporary US-China competition. SSince 2022, the United States Bureau of Industry and Security has employed a fluctuating strategy of tightening and selectively loosening export licensing for advanced AI chips destined for China. By January 2026, this approach transitioned from a general presumption of denial to case-by-case licensing contingent upon

specific supply, security, and testing benchmarks, while simultaneously affirming in mid-2026 that these mandates apply to Chinese-headquartered firms regardless of their international operations. China has countered with its own restrictions on rare earths and critical minerals essential to chip fabrication and clean-energy supply chains. Consequently, any AI-SCRM system monitoring this sector must continuously reassess supplier risk as the regulatory environment evolves; a supplier's compliance status can fluctuate not because of changes in its own conduct, but due to exogenous modifications to licensing thresholds or entity-list designations. This reciprocal weaponization of supply chains forces firms to adopt dynamic compliance architectures that can rapidly recalibrate their risk profiles in response to these sudden shifts in export-control regimes (Chen & Evers, 2023; Farrand, 2024).

Under the proposed framework, such a system would register high Structural Dependency Concentration due to the significant consolidation of advanced lithography and foundry capacity among a limited set of firms and jurisdictions, notably Taiwan, South Korea, and the Netherlands (Aguirre, 2024; Ou et al., 2024). It would also likely exhibit elevated Regulatory Fragmentation Risk, as operational compliance necessitates navigating overlapping mandates: US export controls and entity lists, Chinese data-security and retaliation measures, and the European Union's AI Act risk classifications for critical infrastructure. In this sector, Algorithmic Bias Exposure appears less a consequence of supplier scale than a manifestation of asymmetric data availability; Chinese domestic suppliers are often less visible to Western-trained models than incumbent Taiwanese or South Korean firms, which can result in systematically compromised risk assessments in domains marked by heightened geopolitical volatility (Zhang & Zhang, 2023).

For a middle power such as India, positioned as neither a principal architect of export-control policy nor a primary target of it, but increasingly courted as an alternative node in semiconductor and electronics assembly supply chains.The framework suggests a distinct strategic posture: Indian firms and regulators adopting AI-SCRM systems must rigorously weigh Regulatory Fragmentation Risk and Structural Dependency Concentration in vendor selection. This strategic emphasis is crucial for safeguarding India's interoperability with both US-aligned and non-aligned supply networks, thereby enabling its role as an alternative node and preventing premature bloc alignment.

3.4 Positioning Against Current Regulatory Regimes

The proposed evaluative framework elucidates the divergent conceptualizations of risk underpinning contemporary artificial intelligence regulatory regimes. The European Union's AI Act, having entered into force in August 2024 with phased application through 2026, utilizes a graduated, risk-based taxonomy. This legislative instrument prioritizes the mitigation of algorithmic harm specifically encompassing bias within high-risk classification systems as the central objective of regulatory oversight.

This regulatory strategy corresponds most directly with the framework's ABE dimension. Conversely, United States AI governance predominantly operates via supply chain-focused mechanisms, such as export controls and entity-list designations, thereby aligning with the SDC and DSP dimensions. China's regulatory framework concerning data security and personal information protection emphasizes data localization and state access; this orientation effectively reorients the European Union's rights-centric paradigm toward a sovereignty-focused objective.

This outcome underscores the operational constraints of the algorithmic sovereignty trilemma: given that simultaneous compliance with these distinct regulatory philosophies is economically prohibitive, multinational enterprises are increasingly adopting jurisdictionally segmented, parallel AI architectures in lieu of monolithic global systems.

4. Discussion

The implications of the findings detailed in Section 3 extend well beyond the immediate context of semiconductor and critical-minerals supply chains, or the narrow confines of existing AI-SCRM scholarship. The ensuing analysis categorizes these implications into four key areas: theoretical developments, practical and policy considerations, methodological constraints, and prospective research avenues.

4.1 Theoretical Implications

The algorithmic sovereignty trilemma extends structural realist and power transition reasoning into a domain — the micro-architecture of firm-level information systems that International relations theory has historically excluded this domain from systemic analysis. While classical structural realism prioritizes the distribution of material capabilities among states and power transition theory examines growth differentials between rising and established powers, neither framework directly explains how specific classification algorithms and datasets influence systemic distributions. The proposed trilemma addresses this gap by illustrating how firm-

level design choices aggregate across industries, culminating in the network-level chokepoints and panopticon effects that Farrell and Newman describe as sources of state coercive leverage. This approach offers a partial resolution to the critique that structural realism struggles to explain sub-systemic technological change as anything other than an exogenous shock; it instead treats algorithmic design as an endogenous site where systemic pressures shape firm behavior, which subsequently reinforces systemic structure.

The framework also addresses a persistent dichotomy within the literature on algorithmic fairness. Scholarship in this domain has historically conceptualized bias as a technical deficit remediable via data refinement or rigorous auditing, thereby treating fairness and security as discrete engineering challenges. Conversely, the trilemma posited here suggests that, within the context of cross-border enterprise architectures, these objectives are inextricably linked; security-hardening and bias-mitigation mandates often impose contradictory design requirements. While this observation does not invalidate the normative necessity of bias reduction, it implies that a technocratic fairness agenda, if decoupled from the jurisdictional topography of data pipelines, will inevitably encounter friction from export-control and data-security regimes oriented toward divergent ends. Consequently, integrating International Relations concepts of sovereignty and positional power with the fairness literature's discourse on disparate impact is not merely an exercise in interdisciplinary synthesis, but a foundational requirement for developing a comprehensive understanding of the phenomena under investigation.

4.2 Practical and Policy Implications

For firms operating AI-SCRM systems, the framework's primary contribution is to render the trilemma's trade-offs explicit during system design, rather than allowing them to emerge as reactive compliance crises. A firm that discovers—only following a data-localization mandate or export-control designation—that its risk-scoring architecture necessitates a comprehensive data-pipeline redesign has effectively made an unexamined choice among the trilemma's three legs. The evaluation framework in Table 1 facilitates these strategic choices by rendering them auditable in advance, functioning less as a compliance checklist than as a design-stage diagnostic comparable to a threat model in security engineering.

For regulators, this framework suggests that the current pattern of dimension-specific policy,the European Union's focus on ABE-type harms, the United States' emphasis on SDC-type dependency, and China's prioritization of DSP-type sovereignty is not merely a byproduct of varying national priorities. Instead, it is a structurally predictable outcome of each jurisdiction's position within the trilemma. This presents a clear implication for regulatory design,harmonization initiatives are more likely to succeed when they target a single dimension rather than attempting comprehensive alignment across all three simultaneously.

For middle powers such as India, the analysis in Section 3.3 necessitates a recalibration of procurement and regulatory postures. Rather than pursuing a singular AI-SCRM architecture optimized for a specific leg of the trilemma, firms and regulators situated at the nexus of US-aligned and non-aligned supply networks face a strategic imperative to prioritize interoperability and resilience against regulatory fragmentation. This approach requires sacrificing marginal technical optimization for the architectural flexibility needed to preserve market access across divergent technological blocs. Such a stance aligns with India's broader strategic objective of safeguarding sovereign autonomy and avoiding premature alignment within emerging technology policy spheres. Consequently, domestic AI-governance frameworks should integrate an explicit dependency-concentration metric modeled on the SDC dimension introduced here to supplement conventional, bias-centric approaches like the EU's, which often prove insufficient for navigating the geopolitical complexities of cross-border data architectures. Adopting a risk-management strategy that emphasizes resilience and strategic partnerships allows for more effective navigation of these constraints without necessitating total isolation . In this context, the development of robust, localized digital assets serves as a critical hedge against systemic volatility, ensuring that domestic technological progress remains insulated from the disruptive pressures of shifting geopolitical alliances (Timmers, 2019).

4.4 Directions for Future Research

The limitations discussed above suggest three primary trajectories for future scholarship. First, empirical validation is requisite and subsequent research should assess the proposed indicators using firm-level data gleaned from structured case studies, industry surveys, or regulatory disclosure mandates such as those instituted by the EU AI Act's high-risk system requirements to determine whether the four dimensions operate as empirically distinct constructs or exhibit the collinearity posited by the trilemma. Second, comparative sectoral analysis is necessary. Applying this framework across industries with diverse regulatory profiles such as pharmaceuticals, critical minerals, financial services, and agricultural commodities would determine whether dimension weighting is sector-invariant or requires sector-specific adjustments. Third, a more granular exploration of mitigation strategies is required. Delineating technical architectures that most effectively address specific legs of the

trilemma, while balancing associated costs, would evolve the framework from a diagnostic instrument into a functional design tool for stakeholders and regulators. Finally, examining the political economy of data-intensive innovation through the lens of state-led surveillance AI investments will clarify whether regimes with weaker privacy norms possess an inherent comparative advantage.

5. Conclusions

Reorienting the discourse surrounding artificial intelligence and geopolitics moving beyond the reductive lexicon of a technological arms race toward the structural mechanics of algorithmic governance provides a more robust and policy-relevant research agenda necessary for navigating the complexities of the contemporary global technological order.AI-driven supply chain risk management systems are far from peripheral to great-power competition; rather, they serve as critical operational arenas where abstract strategic rivalries over technological leadership are translated into concrete decisions regarding supplier reliability, cross-border data governance, and the pragmatic application of competing regulatory philosophies. The algorithmic sovereignty trilemma and its four-dimensional evaluation framework offer International Relations scholars and practitioners an essential diagnostic lens for reconceptualizing algorithmic bias and data security, framing them not as mere parameters of engineering compliance, but as foundational structural variables of state power. For middle powers such as India, navigating this volatile landscape renders reliance on standard metrics of accuracy and efficiency insufficient; instead, these actors must prioritize the assessment of AI-SCRM systems through the lens of positional exposure a strategic necessity for preserving sovereign agency within an increasingly bifurcated technological order.Future research must prioritize the empirical validation of these indicators across diverse sectors while fostering a substantive dialogue with policymakers to assess whether targeted, dimension-specific harmonization rather than the pursuit of illusory, comprehensive global standard-setting offers the only pragmatic pathway toward coherent algorithmic governance.

List of Symbols and Abbreviations

AI — Artificial Intelligence; AI-SCRM — AI-Driven Supply Chain Risk Management; ABE — Algorithmic Bias Exposure; DSP — Data Security and Provenance; SDC — Structural Dependency Concentration; RFR — Regulatory Fragmentation Risk; HHI — Herfindahl-Hirschman Index; BIS — Bureau of Industry and Security (United States); IR — International Relations; EU — European Union..

References

1. Abiri, G. (2025). Mutually Assured Deregulation. In *arXiv (Cornell University)*. Cornell University. https://doi.org/10.48550/arxiv.2508.12300
2. Aguirre, T. (2024). On Labs and Fabs: Mapping How Alliances, Acquisitions, and Antitrust are Shaping the Frontier AI Industry. In *arXiv (Cornell University)*. Cornell University. https://doi.org/10.48550/arxiv.2406.01722
3. Almakaty, S. (2026). Algorithmic Diplomacy and the Geopolitics of Artificial Intelligence: Machine-Driven International Relations in a Data-Oriented Global Landscape. In *Preprints.org*. https://doi.org/10.20944/preprints202603.0683.v1
4. Amenitsky, A. V., & Vorobyov, E. G. (2025). Proactive AI risk management. The Second AI Arms Race: From Deregulation to Industrial Policy, Sovereign Infrastructures, and Algorithmic Warfare. *SYNCHROINFO JOURNAL*, *11*(5), 28–33. https://doi.org/10.36724/2664-066x-2025-11-5-28-33
5. Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: a systematic literature review. *AI and Ethics*, *5*(3), 3265–3279. https://doi.org/10.1007/s43681-024-00653-w
6. Beaumier, G., & Cartwright, M. (2023). Cross-Network Weaponization in the Semiconductor Supply Chain. *International Studies Quarterly*, *68*(1). https://doi.org/10.1093/isq/sqae003
7. Birkstedt, T., Minkkinen, M., Tandon, A., & Mäntymäki, M. (2023). AI governance: themes, knowledge gaps and future agendas. *Internet Research*, *33*(7), 133–167. https://doi.org/10.1108/intr-01-2022-0042
8. Chen, L., & Evers, M. (2023). "Wars without Gun Smoke": Global Supply Chains, Power Transitions, and Economic Statecraft. *International Security*, *48*(2), 164–204. https://doi.org/10.1162/isec_a_00473
9. Davies, G., Mison, A., & Ward, R. A. (2024). Cross-disciplinary AI supply chain risk assessment. *International Conference on Cyber Warfare and Security*, *19*(1), 185–190. https://doi.org/10.34190/iccws.19.1.2179
10. de-la-Morena, C. G. (2025). AI, Governance, and Law in Digital Geopolitics. In *Advances in computational intelligence and robotics book series* (pp. 193–218). IGI Global. https://doi.org/10.4018/979-8-3373-4480-5.ch008
11. Djeffal, C., Siewert, M. B., & Wurster, S. (2022). Role of the state and responsibility in governing artificial intelligence: a comparative analysis of AI strategies. *Journal of European Public Policy*, *29*(11), 1799–1821. https://doi.org/10.1080/13501763.2022.2094987
12. Farrand, B. (2024). The Economy–Security Nexus: Risk, Strategic Autonomy and the Regulation of the Semiconductor Supply Chain. *European Journal of Risk Regulation*, *16*(1), 279–293. https://doi.org/10.1017/err.2024.63
13. Fu, A., Zhang, X., Xiong, N., Gao, Y., Wang, H., & Zhang, J. (2020). VFL: A Verifiable Federated Learning With Privacy-Preserving for Big Data in Industrial IoT. *IEEE Transactions on Industrial Informatics*, *18*(5), 3316–3326. https://doi.org/10.1109/tii.2020.3036166

14. Ge, J. (2025). Responsible AI Governance in Military Security: Risk Models, Compliance Metrics, and Strategic Stability. *Open Journal of Social Sciences*, *13*(11), 34–57. https://doi.org/10.4236/jss.2025.1311003
15. Guo, R., & Zhang, B. (2026). From Abstract Threats to Institutional Realities: A Comparative Semantic Network Analysis of AI Securitisation in the US, EU, and China. In *arXiv (Cornell University)*. Cornell University. https://doi.org/10.48550/arxiv.2601.04107
16. Hendrycks, D., Schmidt, E., & Wang, A. (2025). Superintelligence Strategy: Expert Version. *SuperIntelligence - Robotics - Safety & Alignment*, *2*(1). https://doi.org/10.70777/si.v2i1.13961
17. Hu, Z., Zhang, C., & Galligan, D. J. (2025). Technology as Statecraft: Remaking Sovereignty, Security, and Leadership in a Multipolar Age. *Politics and Governance*, *13*. https://doi.org/10.17645/pag.11743
18. Ilyinsky, A. I. (2026). Artificial Intelligence and New Geopolitics: Digital Strategies of Russia, India and Brazil. *Humanities and Social Sciences Bulletin of the Financial University*, *16*(1), 6–14. https://doi.org/10.26794/2226-7867-2026-16-1-6-14
19. Ishkhanyan, A. M. (2025). The sovereignty-internationalism paradox in AI governance: digital federalism and global algorithmic control. *Discover Artificial Intelligence*, *5*(1). https://doi.org/10.1007/s44163-025-00374-x
20. Kilian, K. A. (2024). Beyond Accidents and Misuse: Decoding the Structural Risk Dynamics of Artificial Intelligence. In *arXiv (Cornell University)*. Cornell University. https://doi.org/10.48550/arxiv.2406.14873
21. Klingler-Vidra, R. (2019). AI super-powers: China, Silicon Valley and the new world order. *International Affairs*, *95*(2), 485–486. https://doi.org/10.1093/ia/iiz011
22. LEE, A. (2025). The Conceptual Architecture of Digital Governance: A Systematic Review (2015-2025). *Digital Society & Virtual Governance*, *1*(2), 80–106. https://doi.org/10.6914/esjj0n53
23. Liu, H., & Lin, C.-F. (2025). Techno-Geopolitics and Semi-conductor Chokepoints: beyond the US-China WTO Dispute. *The Journal of World Investment & Trade*, *26*(4), 749–791. https://doi.org/10.1163/22119000-12340372
24. Mügge, D. (2024). EU AI sovereignty: for whom, to what end, and to whose benefit? *Journal of European Public Policy*, *31*(8), 2200–2225. https://doi.org/10.1080/13501763.2024.2318475
25. Muldoon, J., Valdivia, A., & Badger, A. (2025). The politics of artificial intelligence supply chains. *AI & Society*, *41*(2), 1175–1187. https://doi.org/10.1007/s00146-025-02625-y
26. Navarro-Meneses, F. J., & Pablo-Martí, F. (2025). Reimagining human agency in AI-driven futures: a co-evolutionary scenario framework from aviation. *European Journal of Futures Research*, *13*(1). https://doi.org/10.1186/s40309-025-00260-w
27. Ness, S., Singh, N., Volkivskyi, M., & Phia, W. J. (2024). The Application of AI and Computer Science in the Context of International Law and Governance "Opportunities and Challenges." *American Journal of Computing and Engineering*, *7*(1), 26–36. https://doi.org/10.47672/ajce.1878
28. Niikondo, S. M., & Ziezo, M. M. (2026). Capacity-building strategies and policy recommendations for sustainable big data utilization in Namibia's small business sector. *Computer Science & IT Research Journal*, *7*(2), 60–68. https://doi.org/10.51594/csitrj.v7i2.2195
29. Nikolić, D., Stanojević, M., & Azdejković, M. (2025). International security and the geopolitics of industrial and defense technologies. *Megatrend Revija*, *22*(3), 213–224. https://doi.org/10.5937/megrev2503213n
30. Nwachukwu, P. S., Chima, O. K., & Okolo, C. H. (2025). The artificial intelligence governance framework for finance: A control-by-design approach to algorithmic decision-making in accounting. *Finance & Accounting Research Journal*, *7*(8), 350–379. https://doi.org/10.51594/farj.v7i8.2016
31. Oludayo, E. (2024). The Geopolitics of Artificial Intelligence: Power, Leadership, and the US-China Rivalry. *Global Multidisciplinary Perspectives Journal*, *1*(6), 205–213. https://doi.org/10.54660/gmpj.2024.1.6.205-213
32. Ou, S., Yang, Q., & Liu, J. (2024). The global production pattern of the semiconductor industry: an empirical research based on trade network. *Humanities and Social Sciences Communications*, *11*(1). https://doi.org/10.1057/s41599-024-03253-5
33. Paul, R. K. (2023). AI INTEGRATION IN E-COMMERCE BUSINESS MODELS: CASE STUDIES ON AMAZON FBA, AIRBNB, AND TURO OPERATIONS. *American Journal of Advanced Technology and Engineering Solutions*, *3*(3), 1–31. https://doi.org/10.63125/1ekaxx73
34. Rao, G. S. N. (2024). AI-Driven Identification of Critical Dependencies in US-China Technology Supply Chains: Implications for Economic Security Policy. *Journal of Advanced Computing Systems*, *4*(12), 43–57. https://doi.org/10.69987/jacs.2024.41204
35. Reuel, A., Bucknall, B., Casper, S., Fist, T., Soder, L., Aarne, O., Hammond, L., Ibrahim, L., Chan, A., Wills, P. R., Anderljung, M., Garfinkel, B., Heim, L., Trask, A., Mukobi, G., Schaeffer, R., Baker, M., Hooker, S., Solaiman, I., … Trager, R. (2024). Open Problems in Technical AI Governance. In *arXiv (Cornell University)*. Cornell University. https://doi.org/10.48550/arxiv.2407.14981
36. Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: an analysis of statements and policies. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1575
37. Robles, P., & Mallinson, D. J. (2025). Advancing AI governance with a unified theoretical framework: a systematic review. *Perspectives on Public Management and Governance*, *8*(4), 213–227. https://doi.org/10.1093/ppmgov/gvaf013
38. Schmidt, E. W. (2022). AI, Great Power Competition & National Security. *Daedalus*, *151*(2), 288–298. https://doi.org/10.1162/daed_a_01916
39. Schmitt, L. (2021). Mapping global AI governance: a nascent regime in a fragmented landscape. *AI and Ethics*, *2*(2), 303–314. https://doi.org/10.1007/s43681-021-00083-y
40. Srivastava, S., & Bullock, J. B. (2024). AI, Global Governance, and Digital Sovereignty. In *arXiv (Cornell University)*. Cornell University. https://doi.org/10.48550/arxiv.2410.17481

41. Stanojević, N. (2025). Big Data-Driven Approaches to Geopolitical Risk and MNC De-risking Strategies. *Journal of Soft Computing and Decision Analytics*, *3*(1), 112–122. https://doi.org/10.31181/jscda31202563
42. Timmers, P. (2019). Ethics of AI and Cybersecurity When Sovereignty is at Stake. *Minds and Machines*, *29*(4), 635–645. https://doi.org/10.1007/s11023-019-09508-4
43. Tran, H.-C. (2026). Brokerage in the Black Box: Swing States, Strategic Ambiguity, and the Global Politics of AI Governance. In *arXiv (Cornell University)*. Cornell University. https://doi.org/10.48550/arxiv.2601.06412
44. Truby, J., Dahdal, A., Brown, R. D., & Ibrahim, I. A. (2026). Diplomacy in the age of AI: Legal and strategic approaches to techno-nationalism, regulatory soft power and the AI chips race. *University of Twente Research Information*, *12*, 100335–100335. https://doi.org/10.1016/j.resglo.2026.100335
45. Undheim, T. A. (2024). The whack-a-mole governance challenge for AI-enabled synthetic biology: literature review and emerging frameworks. In *Frontiers in Bioengineering and Biotechnology* (Vol. 12, pp. 1359768–1359768). Frontiers Media. https://doi.org/10.3389/fbioe.2024.1359768
46. Vujičić, J. (2024). Algorithmic borders: AI, trade controls, and the rise of extraterritorial enforcement in technology law. *World Journal of Advanced Research and Reviews*, *24*(1), 2769–2774. https://doi.org/10.30574/wjarr.2024.24.1.3129
47. Weymouth, S. (2025). Digital Disintegration: Techno-Blocs and Strategic Sovereignty in the AI Era. *International Organization*, *79*. https://doi.org/10.1017/s0020818325101070
48. Yoon, J., Oh, J., Bae, J., Cheng, T. C. E., & Jung, K. (2026). Export Controls and Strategic Adaptation in AI-Enabling Supply Chains. *IEEE Transactions on Engineering Management*, *73*, 2222–2243. https://doi.org/10.1109/tem.2026.3669349
49. Zhang, J., & Zhang, Z. (2023). Ethics and governance of trustworthy medical artificial intelligence. *BMC Medical Informatics and Decision Making*, *23*(1), 7–7. https://doi.org/10.1186/s12911-023-02103-9