Academic Education Publishing House

Economic Society and Humanities Vol. 3 No. 7, 2026

The Asymmetric Sovereignty Paradigm: Regulatory Divergence and Compliance Inflation in US–China Cross-Border Data Governance

Shengchang Zhang[1,*], Fred Zhang[2]

[1]School of Business Administration, Baise University, Baise, Guangxi, China

[2]Amador Valley High School, Pleasanton, California, USA

**Corresponding Author*

Abstract: The work of uncovering the rising structural tension in international digital trade between China and the United States is conceptualized by this monograph, which uses an analytical paradigm called the Asymmetric Sovereignty Paradigm. The digital economy has fragmented along discrete regulatory geometries even though the traditional trade architectures have been tuned to help in distributing resources across the borders by reducing tariffs at the same time as negotiating access to the market. The American system is based on a decentralized, market-oriented regime encouraging Free Cross-Border Data Flows (CBDF), which is used in defense with national security interventions and extraterritorial enforcement. On the other hand, China has institutionalized a state-based, sovereignty motivated, infrastructure based on inflexible data localization, tiers of outbound screening and the legalization of asset-logging. This paper makes formal the manner in which the convergence of these paradigms of conflict creates systemic inflation of compliance to multinational corporations. We develop the multi-vector optimization model that assesses the structural friction that systemic regimes of data export compliance proposed to China impose on extraterritorial needs of US employment of legal frameworks. The article illustrates the role of regulatory asymmetric trends in the bifurcation of the world-wide technology stack and why global firms must break down integrated enterprise architectures to localized, isolated, data enclaves in order to ensure jurisdictional survivability.

Keywords: Cross-Border Data Flows; Data Sovereignty; Compliance Inflation; Extraterritorial Jurisdiction; Regulatory Asymmetry; Data Localization; Technology Governance

1. Introduction and Theoretical Foundations

The modern macroeconomic environment is becoming more and more determined by competitive patterns of the digital economy. The paradigms of sovereign governance of the two prevailing tech ecosystems, the United States and China, have steadily diverged into irreconcilable structural philosophies in the last few years. The American system traditionally flaunts a liberal, market-focused ideology that assumes that the free, smooth movement of computational data across borderlines results in predictable productivity gains in cross-border efficiency, platform monetization and transnational supply chain orchestration. In this perspective, data transfers are approached as business dealings that need to be excluded to state action, except under narrowly focused and tightly targeted national security requirements, which are handled by specialized solutions [1,2]. On the other hand, the Chinese system of digital governance has experienced a radical change, with a transition to a state-oriented, sovereignty-based paradigm. This model explicitly classifies data as a formal, strategic fifth factor of production, next to the traditional factors of production, like land, labor, and capital and technology [3,4]. Data in this institutional philosophy is not just a short-lived side effect of the trade between individual able businesses, but the crude content of national sovereignty and macroeconomic stability. The state-directed approach, in light of the changing geopolitical environment, has created a complex compliance grid, which is aimed at preventing the unauthorized exfiltration of important information resources and forcibly drives domestic storage, processing, and localized alignment [5,6].

This monograph develops an analytical paradigm called the Asymmetric Sovereignty Paradigm to examine structural friction by these conflicting paths. Conventional models of international relations usually view regulatory alignment as a coordination game that is linear in nature and that sovereign actors will ultimately meet on common standards in order to eradicate market friction. This assumption is questioned in Asymmetric Sovereignty Paradigm that shows how opposing legal concepts of ownership of data, national security level and jurisdictional boundaries, generate structural barriers that are permanent and non-convergent. This regulatory mismatch compels international business to conduct their business within a framework whereby being able to please the regulatory requirements of one jurisdiction automatically places the organization to be under legal liability or even an operational lockdown in the other jurisdiction [1,7].

2. Free-Flow Market Doctrine vs. States Data Sovereignty

The methodical conflict in transnational digital trade is based on the theoretically incompatible regulatory constructions. Limit the final operation speed of a cross-border digital framework, gauged through institutional transaction friction F, institutional localization needs L, and the degree of extraterritorial jurisdiction J. The common expression of this geometrical friction can take the shape of a multipower-law expression:

$$F(R, L, J) = \left(\frac{R_c}{R}\right)^{\alpha_R} + \left(\frac{L_c}{L}\right)^{\alpha_L} + \left(\frac{J_c}{J}\right)^{\alpha_J} \quad (1)$$

And αR, alphaL, alphaJ are exponents of institutional friction and Rc, Lc, Jc are empirical compliance constants at the base. In this formulation, the global frontier would need to make exponential increases in regulatory compliance costs, local legal frameworks, and sovereign clouds in parallel to have a seamless cross-border interoperability. This fact has compelled foreign business compliance spending to great heights. In 2025, multinational corporations in the US-China corridor were spending corporate capital on digital compliance, segregation of local data, and dual-stack server architecture alone as a direct result of multinational corporations reached a total of tens of billions of dollars annually [8]. This monopoly establishes a structural separation together with an obstacle to entry, turning worldwide digital business into a sector that caters to corporate entities that can absorb the compliance friction in the system. This severe policing division is however challenged with structural barriers that are critical. The unrestricted commercial pipelines that form the basis of the software-as-a-service (SaaS) and cross-border digital ecosystems of the world are starting to meet an obstacle in the form of regulation. There is an opinion among legal experts that the absolute cross-border compatibility of unsegregated, multi-tenant databases will be seriously limited at the end of the 2020s as a result of increasing national security requirements [1,5]. When broad-based data interoperability is flattened, the nature of international operation moves towards a hyper-localized data siloing, edge-based processing, and isolated network enclave, where enterprises must sacrifice world-data centralization, in order to exist as fully localized compliance islands.

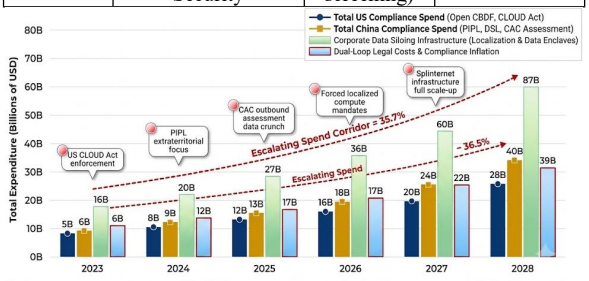
The Chinese strategic paradigm implements this paradigm of boundaries-first by a very integrated tiered regulatory ecosystem. Instead of taking the laissez-faire position in relation to commercial data exfiltration, Chinese officials have institutionalized a very stringent state-vetted pipeline outbound transfer. Well-established regulatory bodies issue binding security requirements that compel organizations that process sensitive or high volume personal information to pass security inspections by the state before any cross-border transmission is effected [6,9]. By the end of 2025, multinational companies with operations in China had switched in large numbers, away to local server nodes, as the implementation of the data export compliance measures by China forced them to change. The overall regulatory approaches and the compliance architecture efficiencies are summarized in Table 1.

The figure 1 shows the gradual increase in the corporate compliance and data siloing infrastructure spending that is expected to rise on the US-China corridor. With the conflicting application of regulations like the US CLOUD Act and the Chinese data export laws (PIPL and CAC tests), multinational companies are under pressure of a cross-jurisdictional squeeze. In order to reduce legal risks, international companies are being compelled to leave cost-effective, centralized multi-tenant data stores and migrate towards regionalized data enclaves

and isolated regional server nodes. As the expected cost of expenditure continues to be high, the economic cost of sustaining parallel tech stacks, bi-polar legal framework, and localized compute environments is shifting regulatory compliance out of the corporate cost overhead to an emerging obstacle in worldwide digital integration [8,10].

Table 1. Regulatory Strategy Versus Compliance Architecture Efficiency

Paradigm Strategy	Primary Regulatory Vector	Compliance Friction	Interoperability
Liberal Free-Flow	Market Monetization & Free CBDF	Low (Targeted review)	High (Open)
Sovereignty -Centric	State-Vetted Localization & Security	High (Mandatory screening)	Restricted



Projections assume sustained geopolitical friction and mandatory localized architectures (Scenario C). See Chapter 4 for detailed model parameters. Data adapted from Figure 1 data (CAICT, STAN HAI HAI report, and OECD).

Figure 1. Corporate Compliance & Data Siloing Infrastructure Spend Multi-Year Projections

3. The Structural Mechanics of China's Data Export Framework

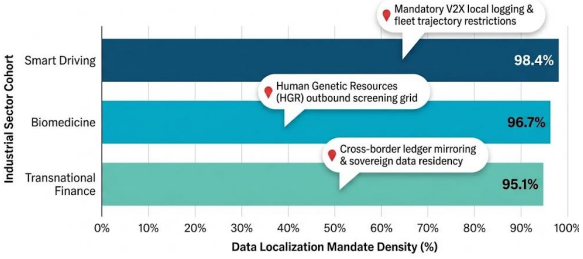
The second and more consequential element of the paradigm of asymmetric sovereignty lies in the statutory dynamics of the Chinese system of extensive regulatory grid. The policy guidelines of the central policy of China literally codify the pipeline of data export using three different legal channels, which form a uniform template of compliance to all cross-border digital flows. These channels are imposed according to the volume of data processed and strategic level of the organization carrying out the action through institutional guidance of the authorities like Cyberspace Administration of China (CAC) [6,9]. This institutional design creates a three pronged (compliance grid) which is unambiguous:

$$\Omega_{\{export\}} = \Psi \cdot (ACAC \cdot SSCC \cdot CCert)^{\gamma} \Delta t \quad (2)$$

And Ω export is the volume of legally compliant transfer of outbound data, Ψ is the density of systemic regulation, ACAC is the volume of data subject to mandatory CAC Security Assessment, SSCC is the transactions that are subject to Standard Contractual Clauses, CCert is the utilization of the formalized Cross-Border Personal Information Transfer Certification route, and γ is the scaling coefficient of cross-border enterprise operations. This modelling equation streamlines the specific regulatory paths that businesses should follow. To Critical Information Infrastructure Operators (CIIO) or any other party involved in managing masses of personal records of citizens, the obligatory CAC Security Assessment is an insurmountable statutory obstacle. Smaller commercial organizations make use of the framework of Standard Contractual Clauses (SCC) to set up a binding contractual data protection bottom line. The formalized Certification Route offers multinational corporations with a different route of internal corporate transfers, and it introduces a pipeline of certified compliance to coordinate integrated cross-border operations [5,9,11]. Table 2 shows a verification data compliance matrix (empirically) between industrial cohorts.

Table 2. Valid Data Conformity Matrix of Data Comparison among Industrial Cohorts

Industrial Sector Cohort	Localization Density	Compliance Overhead	Rejection Pressure
Smart Driving & Telematics	Very High	High	Elevated
Biomedical & Genomic Research	Very High	High	Elevated
Transnational Financial Services	High	High	Notable



Data reflects administrative mandate density metrics compiled across active regulatory corridor oversight frameworks as of 2026.

Figure 2. Visual Representation of Data Localization Mandate Intensity by Industry Sector

In Figure 2, a regulatory approach is identified where a sovereign organization can impose close to absolute data residency on data-intensive, high stakes, industries. Instead of horizontal compliance rules, the US-China corridor of regulation enforcers implements super-specific vertical measures. The density rate is high in Smart Driving sector due to the high-level of national security classification of vehicles telemetry, high-definition mapping and fleet trajectory logs. Likewise, the Biomedicine and Transnational finance sectors are experiencing tremendous pressures of localization because of the sensitivity of the human genetic resources

and governance ledger issues. In the case of multinational enterprises operating between these clusters, such a high level of density of administrative directives can no longer allow partial compliance and have to be structurally compartmentalized in terms of jurisdiction, leading to the duplication of infrastructure permanently and technological silos on local level [6,9].

4. Compliance Inflation, Extraterritorial Jurisdiction, the CLOUD Act

To safeguard national digital property and assert sovereign power internationally, the United States has designed advanced extraterritorial legal mechanism, which directly oppose domestic rules of localization. Instead of limiting legal discovery requirements to physical domestic boundaries, contemporary Western systems are based on legal systems like the Clarifying Lawful Overseas Use of Data (CLOUD) Act. The CLOUD Act of the American legal system stipulates that any technology provider who is under the jurisdiction of the United States should disclose any data under its control, custody, or possession, whether it is physically stored on a server within the United States or in a foreign country [1,10]. V is the legal discovery demand vector that is issued towards a multinational provider. Extraterritorial data access obligation Y is provided through a weighted sum of the jurisdictional ties and systemic control measures that are implemented at the international level of the whole enterprise:

$$Y = \Sigma i \in Jurisdiction\ J(x)\ i \cdot Ci(x) \quad (3)$$

In which J(x) i is the legal probabilities of the nexus of a domestic court with regard to corporate entity x, and Ci(x) is the functional control functions a server asset i is subjected to. By establishing the jurisdictional net very broad, and implementing enforcement of all global subsidiaries, Western regulators break the legal discovery powers of traditional physical geography. This geographical expansion makes sure that the law enforcement access can keep up with the decentralized trends of cloud storage, as well as other systems will be able to systematically undermine the sovereign data limits imposed by other nation-states.

This legal overreach generates a conflagration. In the case when a court in the US requires the provision of customer data stored in China under the CLOUD Act, the target enterprise will be subjected to a serious legal conflict. The submission under the US federal subpoena is a direct breach of the Data Security Law (DSL) and Personal Information Protection Law (PIPL) of China which clearly prohibits the transfer of domestic data to foreign legal or law enforcement agencies without the prior consent of the state [5,9]. This collision leads to an optimization ghetto of corporate legal and technical engineering groups and results in that compliance inflation accelerates as companies build up softwares layers of redundancy and legal insulation that ensure that no data is in cross-border leaked and suffer enforcement of the competing national subpoenas.

5. Technology Architecture Fragmentation and Structural Vulnerabilities

The worldwide spread of divergent data compliance regimes brings about complex technology governance dynamics. When incompatibility sovereign legal frameworks assert themselves as a default operational standard to software deployment across the globe, they systematically influence international technical architectures, database schema designs and enterprise cloud properties. This dynamic produces structural dependencies and fragmentation of infrastructure that is very resistant to the sudden change or integration across borders. Enterprise developers who develop software stacks based on highly segmented database architectures that support localized compliance become trapped in an inflexible environment where re-integrating global data assets requires significant rewriting costs, re-engineering of the architecture and significant operational friction [1,10].

Nonetheless, this decentralized, patented infrastructure design bears wire coded technical weaknesses. International cybersecurity institution engineering assessments have indicated that multi-region compliance schemes, which are fully decoupled and multi-region, pose unique architectural alignment problems and security concerns. As soon as database parameters are localized behind hard, national firewalls, compliance-driven, real-time capabilities to telemetry security and detect threats can be poisoned or beaker-blinded by the filters. This fragmentation does not allow global chief information security officers to continue to have a single view of their entire corporate footprint and allows malicious actors to use

blind spots created by data-localization boundaries, obscure unauthorized exfiltration vectors, or to set up localized infrastructure nodes to conduct covert cyber activities [10,12].

6. Structural Analysis of Global Digital Governance Frameworks

Another complication is that the international multi-lateral trade policies have found it difficult to co-exist with the growth in regulatory coherence as the asymmetric sovereignty mechanism increasingly makes the open market diffusion process conflicting with the state-centric localization process. Previously, the regimes of technology control around the world worked on the premise that restricting access to physical elements of capital, namely, advanced hardware, transoceanic fiber cables, and physical data center nodes, would create a powerful defensive barrier. This conventional trade model considers data as a by-product that simply adheres to the constraints of deployment of the underlying hardware networks [8].

This dependency map is completely reversed by the emergence of a complexly designed data sovereignty law. When implemented systematically, frontier-level data governance regimes rewrite the software engineering principles of the global commerce ecosystem, and make the realization of global (unified) cloud networks low-order less useful in the long term. E.g. a single, unreplicated worldwide consumer database with conventional multi-tenant cloud architecture would need a fraction of the energy and capital footprint needed to operate multi-region, zero-trust isolated enclaves. As a result, the lack of downstream regulatory fragmentation cannot be avoided by traditional multi-lateral trade agreements, which means that the conventional open-market rules become more and more incomplete as a global digital economy regulation tool [1,5].

7. Empirical Projections and Multi-Pathway Scenarios

As a way of tracing out the path of this strategic cross-border data friction to 2030, we simulate three different technological and regulatory futures depending on the interactions of a market-driven free flows and state-centric localization loops. Scenario A (The Global Multilateral Convergence) supposes that international trade institutions are able to reach a deal whereby the world has a unified and global data governance system which is able to establish standardized terms of cross-border contracts, harmonized definitions of security, and mutual legal assistance agreements, reducing the absolute compliance cost to the point that integrated global cloud systems are still viable in terms of their commercial viability. Standardized reciprocity, in this case, is a long-term alleviation of economic friction in the system.

Scenario B (The Total Fractured Splinternet) supposes that barriers to national data sovereignty become an irrevocable, geopolitical wall in 2027. Under this route, increment of marginal compliance is very prohibitive to an extent that multinational corporations are compelled to perform a wholesome operational decoupling. At the same time, big tech giants completely ban foreign-origin software, cloud-computing and data-processing systems in their home countries, turning the world wide web into a network of fully closed, ideologically homogenous national intranets that block any non-vetted cross-border data transfer [1]. The Bifurcated Asymmetry Enclave (Scenario C) is a structural embodiment of the Asymmetric Sovereignty Paradigm. In this case, the global digital economy has continued to have a deeply networked layer of non-sensitive commercial flows, simple transactional messages and unrestricted repositories of public texts. Meanwhile, the system provides full architectural isolation of high value strategic segments, such as autonomous transit telemetry, exceptional biometrics, industrial IoT logs, and vital infrastructure metadata. This structural bifurcation formulates a complicated dependency queue in which world corporate tactics are structurally obliged to act through separate, ring-fenced data enclaves, created to fulfill competing sovereign command and control at the same time whilst ensuring just a bare minimum of international operational coordination [5,6].

Figure 3 project the multi-pathway predictive trajectories which specify the structural degradation of the frequencies of global cross-border database synchronization. The lines illustrate two different geo-technological futures beginning at the level in 2024. In Scenario B (Total Fractured Splinternet) the lack of administrative friction and gridlock of all of the regulations leads to a drastic collapse of interoperability, and the index plummets sharply,

as protocol decoupling is utilized completely by 2030. In contrast, Scenario C (Bifurcated Asymmetry Enclave) is an institutional stabilization, pragmatic in nature. Although it represents an irreversible decrease in the fluidity of databases in the world in comparison with the past levels, it creates a working balance. In this case, multinational companies obtain predictability in their operations through having completely segregated parallel tech stacks, that are fully aligned with regional data requirements.

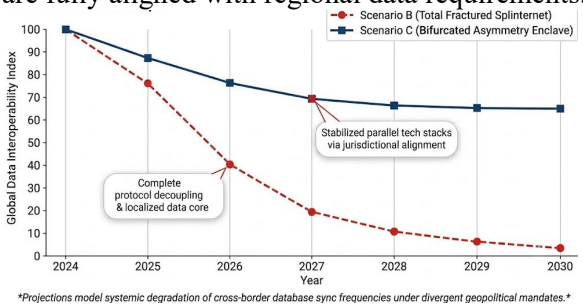


Figure 3. Global Data Interoperability Predictive Models through 2030

8. Conclusion and Policy Recommendations

The Sino-American conflict about the data compliance and digital governance across borders proves that technical and economic leadership cannot be measured with precise market capitalization and the idea of single connectivity. This paper will formalize the Asymmetric Sovereignty Paradigm to show how the combination of strategic commitment to data localization and tiers of export screening by China, with the extraterritorial effect of US legal requirements on the international digital economy has created a secondary and much more fragmented route to the global digital economy. To move around this scenery, corporate boards and global policymakers should have a new form of governance - one that squarely acknowledges the cumulative cost of compliance inflation, the fallacy of global digital convergence, and changes technological landscape to be structurally survivable, zero-trust data compartmentalization, and operational resilience.

The following could be valuable priorities to policymakers and corporate strategists:

(1) Accept compliance inflation as the structural cost of US China digital corridor business and anticipate permanent dual-stack infrastructure investments.

(2) Establish explicit internal decision-making structures on how to categorize data in terms of sensitivity and jurisdictional risk, in order to be able to localize selectively, but not universally.

(3) Favor discriminatory international cooperation on mutual legal assistance and common contractual terms but admit that overall convergence in the law is in the near term.

References

[1] Chander, A. The coming Splinternet? Data nationalism and the fragmentation of the global digital economy. Harvard Law Review, 2020, 133(4): 1122–1145.

[2] Luong, N. Two loops: How China's open AI strategy reinforces its industrial dominance. Research Working Group Paper, U.S.-China Economic and Security Review Commission, 2026.

[3] Ding, J. The diffusion deficit in scientific and technological power: Re-assessing China's rise. Working Paper Series, Centre for the Governance of AI, 2022.

[4] OECD. OECD Digital Economy Outlook 2020. OECD Publishing, 2020.

[5] Erie, M. S., Streinz, T. The Beijing Effect: China's Digital Silk Road as transnational data governance. New York University Journal of International Law and Politics, 2021, 54(1): 1–92.

[6] Kokas, A. Trafficking Data: How China Is Winning the Battle for Digital Sovereignty. Oxford University Press, 2022.

[7] Gao, H. Data sovereignty vs. data free flow: The changing landscape of international data governance regimes. Journal of International Economic Law, 2023, 26(2): 245–268.

[8] National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0) and related guidance on cross-jurisdictional cloud architectures. U.S. Department of Commerce, 2023.

[9] Xu, W., et al. Whose victory? A perspective on shifts in US-China cross-border data flow rules in the AI era. The Pacific Review, 2025, 38(6): 963–989.

[10] Kalash, S. Y. Cross-border data transfer regimes: Current landscape and outlook ahead. CIGI Papers No. 350, Centre for International Governance Innovation, 2026.

[11] Rong, Z. Comparative analysis of cross-border data flow policies: EU, US, and China. 2025 IEEE 24th International Conference on Trust, Security and Privacy in Computing and Communications

(TrustCom), 2025: 2413–2418.
[12]Harrell, P. Managing the risks of China's access to U.S. data and control of software and connected technology. Carnegie Endowment for International Peace, 2025.