Politics and Governance
2025 • Volume 13 • Article 10437
https://doi.org/10.17645/pag.10437

cogitatio

ARTICLE

Open Access Journal

Offshore Embeddedness Beyond the Wall: Chinese Cloud Providers in Southeast Asia's Data Governance Landscape

Binyi Yang and Mingjiang Li

S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore

Correspondence: Binyi Yang (binyi001@e.ntu.edu.sg)

Submitted: 30 March 2025 **Accepted:** 10 July 2025 **Published:** 19 August 2025

Issue: This article is part of the issue "The Geopolitics of Transnational Data Governance" edited by Xinchuchu Gao (University of Lincoln) and Xuechen Chen (Northeastern University London), fully open access at https://doi.org/10.17645/pag.i437

Abstract

Why do middle power states permit companies from institutionally controversial jurisdictions to build and run critical cloud infrastructure on their soil, despite pronounced data governance concerns? How do such firms convert deep suspicion into durable market legitimacy amid intensifying geopolitical competition? Drawing on case studies of Alibaba Cloud and Tencent Cloud across five ASEAN countries (2015–2024), this article proposes the concept of offshore embeddedness: a legitimacy strategy that combines demonstrable separation from home-state control with deep integration into host-state governance structures. Three mechanisms underpin this strategy: regulatory-infrastructure convergence through exhaustive certification and sovereign cloud builds, network integration via stakeholder coalitions that fuse firm survival to domestic political interests, and organizational decoupling accomplished through verifiable legal separation from home-country governance. ASEAN governments shape these outcomes by acting as gatekeeper-regulators (imposing localization and audit preconditions), infrastructure brokers (exchanging market access for domestic data center investment and skills transfer), and coalition orchestrators (embedding foreign clouds within host-led political-economic networks). Through these roles, domestic data governance frameworks shift from exclusionary shields to leverage tools, recalibrating digital governance and binary US–China narratives.

Keywords

ASEAN; Chinese cloud providers; data governance; offshore embeddedness; US–China technological competition

1. Introduction

Data now functions less like a raw production factor and more like a strategic asset, whose custody defines the boundaries of sovereignty, much as the control of sea lanes once did (Chander & Lê, 2014; Ding & Dafoe, 2021). This revaluation has turned rules over storage, processing, and cross-border transfer into prime instruments of statecraft, situating data governance at the center of contemporary great-power competition (X. Chen & Gao, 2024; Christophe et al., 2023; Tang, 2020). Washington and Beijing each leverage export-control lists, security reviews, and market-access vetoes to constrain the other's cloud champions, framing foreign platforms as vectors of surveillance or coercion. Yet, multinational enterprises continue to thread operations through this tightening lattice of restrictions, and—critically—Southeast Asian governments do more than passively watch the contest unfold. How can firms whose home jurisdictions are framed as security risks secure legitimacy abroad, and must ASEAN states merely choose sides, or can they wield domestic data governance clauses to extract investment, technology transfer, and political leverage from competing cloud providers? The rapid ascent of Alibaba Cloud and Tencent Cloud across major ASEAN markets offers a revealing vantage point for answering these questions.

Despite entering the ASEAN market later than Western counterparts, Chinese cloud providers have rapidly expanded their data centers across the region, now outpacing American competitors in physical presence (K. Xu, 2023). Alibaba Cloud and Tencent Cloud currently operate data centers in Thailand, Malaysia, Singapore, and Indonesia, with Alibaba additionally maintaining facilities in the Philippines—a country with ongoing maritime disputes with Beijing and a historically US-aligned stance. In contrast, Amazon Web Services (AWS) operates data centers in Singapore and Indonesia, while its Thailand and Malaysia facilities remain under development. Microsoft Azure maintains a presence in Singapore, with locations in Indonesia and Malaysia pending deployment. Alibaba Cloud's market share in Southeast Asia increased substantially from 3.7% in 2018 to 15.2% in 2023 (Chai, 2024).

These gains were achieved in jurisdictions that explicitly invoke data sovereignty principles to justify localization mandates, licensing requirements, and security audits. While ASEAN governments have not established a shared definition of "data sovereignty," this article uses the term to refer to the assertion of national jurisdiction over data generated within territorial borders, typically implemented through local storage mandates, cross-border transfer restrictions, and national security exemptions that enable governments to control the cross-border movement of data. Indonesian officials have characterized digital sovereignty as essential to preventing digital colonization ("Minister calls for protection," 2022). Vietnam's Cybersecurity Decree 53/2022 mandates in-country storage of regulated data, establishing data localization as a government enforcement mechanism (The Government of Vietnam, 2022). Malaysia's MyDIGITAL blueprint prioritizes building a trusted and secure digital environment, linking cybersecurity to domestic capacity development (Ministry of Communications and Digital, 2021). Thailand requires cross-border data transfers only to destinations with adequate protection standards (Herbert Smith Freehills, 2024), while Singapore mandates comparable protection standards for overseas transfers (Minister for Communications and Information, 2021). These frameworks reflect a regional approach where data governance serves multiple policy objectives beyond privacy protection, creating complex compliance environments for foreign cloud providers. This prompts us to consider the following question: How do Chinese cloud providers achieve market success in ASEAN jurisdictions that have adopted data localization and sovereignty measures often used to curb foreign digital influence?

Three pieces of literature address the presented question but leave it unresolved. International business scholarship explains foreign success through dual embeddedness—cultivating host ties while leveraging home networks (Kostova & Zaheer, 1999; Sun et al., 2012)—yet assumes that institutional distance is bridgeable through firm adaptation, not that home-state laws like China's 2017 Intelligence Law create ongoing sovereignty concerns no conventional strategy can offset. Weaponized interdependence theory shows how hub states exploit network centralities to coerce others (Farrell & Newman, 2019), but it treats firms as passive conduits rather than strategic actors. Polycentric governance research maps how authority disperses across overlapping institutions (Aguerre, 2024; Han, 2024; Kausche & Weiss, 2024), yet it assumes already-legitimate actors and leaves unanswered how controversial-origin firms can convert institutional liabilities into host-state legitimacy.

This article introduces offshore embeddedness: a legitimacy strategy combining demonstrable separation from home-state control with deep integration into host-state governance structures. Through an analysis of Chinese cloud providers across ASEAN's regulatory landscape, we identify three mechanisms that enable firms of controversial origin to transform regulatory scrutiny into a competitive positioning in cloud markets.

2. Controversial Origins and Regulatory Complexity: Chinese Cloud Providers in ASEAN

2.1. Positioning Controversial Origins of Chinese Cloud Providers in its Overseas Expansions

Chinese cloud providers originate from institutional contexts that generate legitimacy deficits in host markets. Three interconnected factors explain why these firms encounter heightened scrutiny that Western competitors avoid.

State-centric data governance conflicts with liberal privacy norms. China's cyber sovereignty framework treats information flows as state territory, subject to party-state oversight, which fundamentally diverges from liberal governance models that emphasize individual rights and consent-based processing (Arner et al., 2022; Gao, 2022). The 2017 Cybersecurity Law operationalized this doctrine through mandatory local storage requirements, creating tensions when Chinese providers enter markets governed by liberal privacy frameworks.

Blurred state-business boundaries raise corporate independence questions. Communist Party committees embedded within nominally private firms create organizational forms where commercial independence and political guidance coexist, challenging traditional public-private distinctions (Pearson et al., 2022). Recent Chinese legal frameworks establish broad expectations that enterprises assist with intelligence work and comply with cross-border data restrictions, making credible demonstrations of state separation difficult in foreign markets that prize corporate autonomy.

Geopolitical competition amplifies technological suspicion. US–China competition has transformed cloud services from commercial offerings into national security considerations, as manifested through initiatives like the Clean Network program, which targets Chinese firms across over 50 countries (Rithmire & Han, 2021). This competitive dynamic means Chinese providers must navigate not only regulatory requirements but broader questions about technological alignment in an increasingly polarized environment.

2.2. ASEAN's Data Governance Landscape

ASEAN's cloud market has expanded significantly in recent years, with public cloud revenues rising by 31.63% since 2019—surpassing the global average of 26.43% (Suruga, 2023). Yet, this surge in market opportunity coexists with a complex regulatory mosaic across member states, which creates substantial legitimacy challenges for foreign cloud providers, particularly those from controversial institutional contexts.

While ASEAN represents a coherent regional economic space with shared digitization goals, the data governance landscape remains highly diversified across member states, creating both challenges and strategic opportunities for multinational cloud providers. Figure 1 highlights substantial variation in both digital trade and data governance metrics, using composite indicators from the Global Data Barometer and Digital Trade Provisions Index. These indicators measure data governance readiness through a weighted aggregation of privacy safeguards, enforcement capabilities, and transparency provisions. The scores range from Singapore's comparatively high overall rating (60%) to Vietnam's more restrictive design (32%), illustrating the regulatory heterogeneity that characterizes the region.

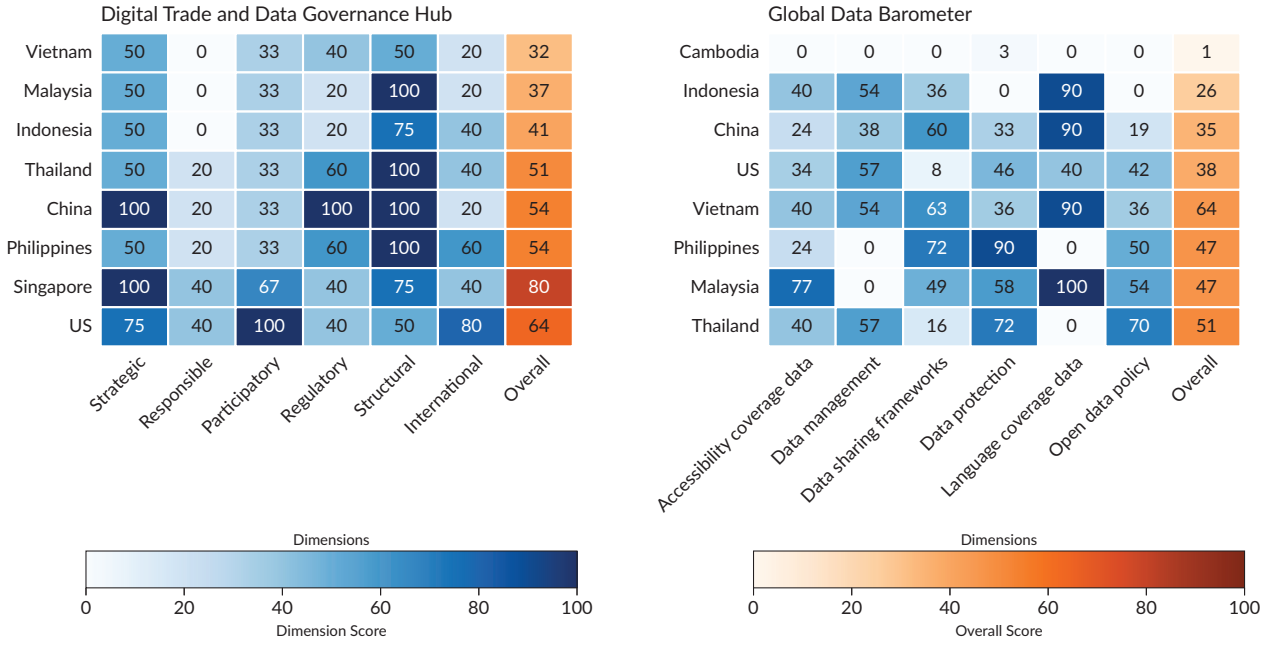

Figure 1. Comparative data governance scores in ASEAN and benchmark countries. Note: Data drawn from the first edition of the Global Data Barometer (2021) and the Digital Trade and Data Governance Hub (2024), selected for their comprehensive ASEAN coverage.

ASEAN's regulatory architecture reveals three characteristics that shape foreign cloud provider operations. Western-influenced governance standards remain deeply embedded across ASEAN, evident in General Data Protection Regulation (GDPR) derived consent-based models and breach-notification requirements in countries such as Malaysia, Singapore, and Thailand (see Supplementary File, Table 1). These frameworks reflect liberal governance philosophies emphasizing individual privacy rights and data subject control. Jurisdictional fragmentation creates complex compliance matrices through regulatory heterogeneity—Indonesia's targeted localization mandates in finance, Vietnam's comprehensive requirements for in-country storage of personal data, and Singapore's permissive approach to cross-border transfers secured by binding

corporate rules. Credible enforcement capacity demonstrates real consequences, as ASEAN regulators possess both legal authority and technical capacity to impose meaningful compliance requirements. Recent enforcement actions demonstrate regulatory capacity: Indonesia blocked major platforms, including Steam and PayPal, for license violations in 2022; Singapore's Personal Data Protection Commission imposed multiple fines on telecommunications providers; and Vietnam conducted comprehensive inspections of TikTok operations in 2023, demanding structural changes.

The intersection of controversial origins with ASEAN's regulatory characteristics creates verification requirements extending beyond routine compliance. Western-influenced standards intensify doctrinal conflicts, requiring Chinese providers to demonstrate credible separation from home-country governance approaches. Jurisdictional fragmentation multiplies verification points, as each jurisdiction applies distinct standards for evaluating independence claims regarding National Intelligence Law obligations and party committee presence. Enforcement capacity creates heightened scrutiny risks where regulatory concerns intersect with geopolitical competition dynamics, precisely targeting the institutional characteristics that define Chinese providers' controversial origins.

3. Literature Review

International business research has long recognized that institutional distance between home and host countries creates systematic barriers for multinational enterprises expanding overseas. Institutional distance encompasses regulatory compliance costs, normative misalignment, and cognitive difficulties in navigating unfamiliar business environments, creating what Kostova and Zaheer (1999) term the "liability of foreignness"—disadvantages faced by foreign firms compared to domestic competitors. These barriers manifest through increased transaction costs, reduced legitimacy with local stakeholders, and difficulties accessing critical resources and information networks (D. Xu & Shenkar, 2002; Zaheer, 1995).

The dominant theoretical solution involves embeddedness and localization strategies that simultaneously cultivate dense ties to host institutions while retaining strong intra-multinational enterprise and home-government linkages to neutralize foreignness penalties. Host-side political and social ties buffer institutional risk by providing access to local knowledge, regulatory influence, and stakeholder networks (Sun et al., 2012). Internal-external embeddedness enhances subsidiary influence and innovation performance through knowledge transfer and resource access (Ciabuschi et al., 2014). This strategic approach assumes that institutional distance represents a bridgeable gap requiring appropriate firm-level responses rather than insurmountable structural barriers.

Research on Chinese firms specifically demonstrates how political connections can facilitate international expansion through multiple channels. Muellner et al. (2017) show that foreign subsidiaries can compensate for institutional disadvantages by integrating deeply into host-country political and social networks, gaining access to local decision-makers, and reducing regulatory uncertainty. Li et al. (2018) demonstrate that Chinese firms with stronger political ties to home governments can better access and leverage intergovernmental diplomatic connections, thereby gaining enhanced access to information, reduced political risks, and increased legitimacy in host countries. These connections operate through formal diplomatic channels, business associations, and informal networks that span public and private sectors.

However, recent research challenges the assumption that political connections provide universal benefits across all institutional contexts. L. Chen et al. (2018) reveal that the efficacy of political networking depends critically on complementary conditions, including firm resources, industry dynamics, and the specific level of institutional distance involved. Their configurational analysis of Chinese high-tech firms demonstrates that different combinations of home political connections, host political connections, research and development capabilities, and internationalization experience are required to overcome high versus low institutional distance. They find that political connections can switch from valuable assets to dispensable strategies—or even liabilities—depending on the institutional context, challenging linear assumptions about distance effects.

This configurational logic suggests that successful international expansion requires a combination of political strategies and firm capabilities, rather than relying on individual solutions. Yet even this sophisticated understanding still presumes that origin represents a manageable handicap once appropriate strategic combinations are deployed—an assumption that breaks down when home-state laws create ongoing sovereignty concerns that no conventional localization strategy can offset.

Weaponized interdependence theory offers a different explanation for multinational enterprise success that shifts the focus from firm-level adaptation to structural network positions under the current geopolitical competition. Farrell and Newman (2019) demonstrate that digital networks exhibit highly centralized structures where states with jurisdiction over central nodes can leverage their positions for strategic advantage through surveillance capabilities and access denial mechanisms. This framework predicts that power flows from hub states, which control network infrastructure, to spoke-states that are dependent on hub-controlled services, suggesting that firm success in international markets depends fundamentally on the strategic positioning of their home states within global networks, rather than on individual firm capabilities.

The theory has been extended to address bipolar competition between US and Chinese digital networks while maintaining core assumptions about hub-state dominance. Lehdonvirta et al. (2025) show that bipolar competition enables spoke-states to exercise choices unavailable in unipolar structures, yet their analysis suggests these choices primarily reflect great-power competition dynamics rather than independent spoke-state agency. China's digital expansion through initiatives like the Digital Silk Road represents hub-state competition for network control rather than empowerment of third countries, with Chinese technology firms serving as instruments of broader geopolitical strategy (Cheney, 2019; Shen, 2018). From this perspective, Chinese technology firms' international success would be explained by China's growing position as a network hub competing with established US dominance rather than firm-level strategic adaptation.

Recent theoretical developments acknowledge significant complications arising from private infrastructure ownership and corporate autonomy that complicate state weaponization capabilities. Gjesvik (2023) demonstrates that ownership-concentrated networks create inherent tensions between commercial interests and strategic objectives that can limit state weaponization capabilities, as private firms resist directives that conflict with profit maximization. Broeders et al. (2025) show that technology companies exercise considerable autonomy in geopolitical contexts, including active resistance to government pressure when it conflicts with business objectives, challenging assumptions about firms as passive conduits of state power.

This perspective receives further support from research on state-firm coordination variations in Chinese corporate internationalization. Oh and No (2020) provide a nuanced framework for understanding the varied patterns of state-firm coordination in China's corporate internationalization, arguing that outcomes depend on complex interactions between firms' foreign direct investment motives and the technology intensity of target industries. Their research on Chinese mergers and acquisitions in Southeast Asia demonstrates that while some transactions involve strong state partnership with elaborate policies and financing, others show more limited alignment or even minimal engagement, supporting the view that Chinese private firms operate as hybrid entities leveraging home-country backing while navigating local sovereignty expectations rather than simply implementing state directives.

He (2024) finds that Chinese technology firms in Indonesia primarily respond to local market conditions rather than implementing state directives, suggesting that commercial adaptation continues to drive firm behavior even in politically sensitive contexts. Yet this framework's emphasis on network topology and hub-state capabilities provides inadequate attention to spoke-state regulatory resources and how these might be leveraged to influence firm behavior. When spoke-states possess significant market opportunities, regulatory authority, or strategic positioning, they may exercise influence that exceeds what network centrality alone would predict, revealing fundamental limitations in both firm-centric international business approaches and state-centric network theories.

Recognizing these limitations, polycentric data governance theory emerged to explain how firms navigate governance authority that is distributed across multiple levels and institutional actors rather than flowing simply from network position or firm adaptation. In polycentric systems, multiple rule-making centers enjoy partial autonomy, adapt to one another, and resolve disputes through shared forums, with no single entity capable of exercising complete control over data flows (McGinnis, 2011; Ostrom, 2010). Aguerre (2024) demonstrates how authority becomes diffused across multiple institutions and jurisdictions in data governance, with overlapping mandates creating institutional complexity where multiple agencies can claim regulatory competence over the same issues.

Firm-level applications reveal dramatically varying outcomes across different jurisdictions and regulatory contexts. Kausche and Weiss (2024) demonstrate how established platforms like Google and Meta successfully captured the EU's Digital Services Act regulatory process through their structural power as digital intermediaries, despite widespread initial demands for strict regulation. Using process-tracing analysis of lobbying activities from 2020 to 2022, they show how these companies leveraged their entrenched position as providers of essential digital infrastructure and employed ideational strategies to shape policy outcomes in their favor, successfully shifting regulatory discourse away from legal accountability toward voluntary responsibility frameworks and preserving technological flexibility by positioning themselves as neutral technical experts.

By contrast, Han (2024) shows how Southeast Asian states exercise strategic agency through selective data localization as economic statecraft, with governments strategically deploying data governance as an economic instrument to achieve political objectives rather than merely responding to security or economic pressures in isolation. Through comparative analysis of Vietnam, Singapore, and Indonesia, Han demonstrates that data localization occurs when states simultaneously experience negative network perception and negative security externalities, with Vietnam's localization reflecting the Communist Party information

control concerns, Singapore's rejection prioritizing its digital hub status, and Indonesia's 2012–2019 policy reversals illustrating evolving state perceptions of technological dependency and security risks.

This framework reveals that state capacity to resist platform power varies significantly based on domestic political calculations within the same global governance system, complicating narratives of either state sovereignty or platform dominance. However, polycentric governance research assumes an arena populated by already-legitimate actors—established Western multinational enterprises in European regulatory processes and long-embedded telecommunications providers in Southeast Asian markets—while treating controversial-origin entrants as analytical afterthoughts rather than central actors requiring theoretical attention.

3.1. Research Gap

None of these explanations fully addresses the empirical puzzle. International business scholarship assumes that institutional distance is bridgeable through conventional adaptation strategies, yet cannot account for cases where home-state laws—such as China's 2017 Intelligence Law—render origin itself a persistent threat that no amount of localization offsets (Kostova & Zaheer, 1999; Sun et al., 2012). Weaponized interdependence theory foregrounds hub-state coercion but reduces firms to passive conduits, underplaying spoke-state regulatory leverage and corporate counter-strategies despite evidence that middle powers and profit-seeking firms continually reshape outcomes (Farrell & Newman, 2019; Gjesvik, 2023).

Polycentric governance research maps distributed authority across multiple actors but assumes an arena populated by already-legitimate incumbents—established Western counterparts and long-embedded telecoms—while treating controversial-origin entrants as analytical afterthoughts (Aguerre, 2024; Han, 2024; Kausche & Weiss, 2024). Consequently, it cannot explain the legitimacy conversion mechanisms we observe in Chinese cloud providers: front-loaded certification, coalition-building with host elites, and multi-tier organizational decoupling that enables data governance screenings and market success across diverse regulatory regimes. Without addressing these gaps, existing frameworks cannot predict why controversial-origin firms succeed where incumbents merely adapt.

4. Methodology

This research employs qualitative comparative case studies with process tracing to examine how Chinese cloud providers operationalize offshore embeddedness across ASEAN's data governance landscape. That, in turn, enables systematic analysis of mechanisms through which controversial-origin firms achieve legitimacy conversion from original liabilities into competitive advantages.

The selection of Alibaba Cloud and Tencent Cloud follows Yin's (2018) theoretical replication logic, testing whether the same framework operates across different organizational contexts. Both share controversial Chinese origins while varying strategically—Alibaba focuses on enterprise digitization through government partnerships, while Tencent emphasizes content services through gaming and entertainment. This variation tests whether offshore embeddedness represents systematic responses to controversial origins rather than firm-specific adaptations. Single-case designs would conflate firm strategies with theoretical mechanisms, limiting generalizability (Eisenhardt & Graebner, 2007).

The five-country design maximizes variation on regulatory stringency while controlling for regional context. Singapore and Malaysia represent mature regulatory environments, Indonesia and Thailand operate as middle-tier regimes, and Vietnam exemplifies restrictive approaches. This systematic variation tests whether mechanisms operate consistently across different regulatory intensities or require specific institutional conditions (Gerring, 2007). Five countries provide sufficient cases to identify patterns while maintaining analytical depth (Ragin, 2014).

Western providers (AWS, Microsoft Azure, and Google Cloud) serve as shadow cases. These firms face identical market opportunities but lack controversial origins, necessitating offshore embeddedness strategies. Shadow case analysis enables identification of which elements represent industry-standard practices versus distinctive responses to legitimacy deficits.

Process tracing examines causal pathways linking institutional challenges to strategic responses to legitimacy outcomes, moving beyond correlation to trace how specific mechanisms generate results (Beach & Pedersen, 2019). Mechanism identification followed iterative analysis across cases and regulatory environments. Initial pattern-matching revealed systematic differences between Chinese and Western approaches. Subsequent analysis clustered these into three coherent strategic responses consistently appearing across firms and markets, then analytically refined these through engagement with our proposed framework.

Analysis draws on corporate documentation (annual reports and regulatory filings), regulatory documentation (national laws and policy announcements), and third-party data (market research and international organizations). The 2015–2024 timeframe captures when Chinese cloud providers started their ASEAN expansions.

5. Analytical Framework: Offshore Embeddedness

5.1. Analytical Foundation: Suchman's Organizational Legitimacy Framework

Suchman's (1995) framework conceptualizes legitimacy as a generalized perception that organizational actions are desirable, proper, or appropriate within socially constructed systems of norms, values, beliefs, and definitions. His framework identifies three legitimacy types: pragmatic legitimacy rests on audience self-interest calculations, moral legitimacy reflects positive normative evaluation of organizational activities, and cognitive legitimacy emerges from comprehensibility and taken-for-grantedness. Suchman addresses legitimacy management through three temporal challenges—gaining, maintaining, and repairing legitimacy through strategic organizational responses.

Building on Suchman's strategic management framework, we identified three core stakeholder questions that controversial-origin firms must address: Can ASEAN regulators believe a Chinese provider will respect their rules? Even if ASEAN regulators trust you technically, who will defend you when politics get rough? And what if Beijing issues an order ASEAN regulators consider incompatible with local requirements? These questions guided our empirical investigation through process-tracing of Alibaba Cloud and Tencent Cloud across five ASEAN markets, producing empirical regularities that pattern-matched into three recurring strategic tasks corresponding to our theoretical questions.

5.2. The Offshore Embeddedness Framework

Offshore embeddedness refers to how controversial-origin firms systematically convert controversial home-country associations into host-state legitimacy assets through simultaneous processes of demonstrable separation from home-country institutional control and deep integration with host-state governance structures and stakeholder networks.

This framework applies when three conditions intersect: institutional controversy, where home-country frameworks may create legal obligations that conflict with host-state sovereignty preferences; business operations involve ongoing access to sensitive data or control over critical digital infrastructure; and host-state regulators possess both the legal authority and technical capacity to monitor and verify organizational separation claims. The framework addresses a security-sensitive legitimacy domain where conventional international business strategies prove insufficient due to heightened suspicion thresholds, persistent security vulnerabilities, and verification imperatives requiring demonstrable rather than communicative evidence of institutional separation.

Guided by three questions inspired by Suchman's (1995) legitimacy theory, the framework rests on three interlocking mechanisms:

1. Compliance signaling through regulatory-infrastructure convergence addresses fundamental credibility deficits by simultaneously pursuing comprehensive certifications and constructing physical infrastructure before revenue justifies such capital expenditure, signaling genuine commitment rather than market opportunism.
2. Network integration via stakeholder coalitions responds to political vulnerability by systematically cultivating financial and reputational stakes among key domestic actors, creating webs of mutual dependence that transform potential adversaries into stakeholders with material interests in continued Chinese presence.
3. Organizational decoupling for jurisdictional assurance addresses core data governance concerns by establishing locally registered entities with genuine legal autonomy, enabling host governments to regulate and enforce against local assets without engaging Chinese parent companies directly.

5.3. Mechanism Analysis

Compliance signaling through regulatory-infrastructure convergence addresses the fundamental credibility deficit facing Chinese technology providers in ASEAN markets. Chinese cloud providers systematically exceed their Western counterparts' regulatory compliance by front-loading both comprehensive certification portfolios and physical data center construction. This strategy diverges from Western incumbents, who typically pursue sequential development—certifying first, then localizing hardware when demand materializes. The simultaneous approach communicates substantial sunk cost commitments to anchor operations under local legal frameworks.

Network integration via stakeholder coalitions manufactures protective coalitions within host countries through direct financial and reputational stakes among government ministries, state-owned enterprises, telecommunications providers, and national champion platforms. Arrangements like Tencent's equity

partnerships with Indonesia's GoTo platform or Alibaba's revenue-sharing agreements in Malaysia's City Brain initiatives create webs of mutual dependence that are costly to unwind, generating Indigenous political protection that transcends formal diplomatic relations.

Organizational decoupling for jurisdictional assurance establishes locally registered entities with genuine legal autonomy, often incorporating local board representation or partnerships with state-linked domestic firms. This structural innovation provides host governments with tangible enforcement mechanisms rather than technical assurances, offering jurisdictional clarity that contrasts with Western providers' reliance on encryption protocols and contractual commitments.

These mechanisms function as complementary layers addressing distinct dimensions of trust and control problems (technical credibility, political backing, and sovereign authority). None alone proves sufficient, but their combination systematically converts Chinese origin from competitive liability into a managed and potentially advantageous market position within ASEAN data governance frameworks.

6. Case Analysis: Offshore Embeddedness in ASEAN's Data Governance Landscape

6.1. Compliance Signaling Through Regulatory-Infrastructure Convergence

Chinese cloud providers neutralize origin-based suspicion in ASEAN by pairing Western-derived compliance with territorially fixed hardware, and by doing so at a greater breadth and speed than their Western counterparts. The mechanism works because it gives regulators a double lock: global best-practice paperwork that they already recognize, plus domestic infrastructure that they can physically police. Drawing on regulation theory (Aglietta, 1979; Lipietz, 1987), capitalist accumulation requires institutional coherence between sectoral strategies and the broader mode of regulation—the ensemble of institutional forms that stabilizes inherently contradictory accumulation processes (Boyer, 2005). When the dominant rulebook for cloud services in ASEAN is a Euro-American compliance assemblage, Chinese providers seek legitimacy by integrating into the status quo. By combining Western-authored certifications with territorially embedded infrastructure, Alibaba Cloud and Tencent Cloud align their operations with the prevailing mode of regulation and thereby neutralize the liability of authoritarian origin.

Procedural convergence comes first. Alibaba became the world's inaugural cloud provider to hold all three Singapore Infocomm Media Development Authority data-protection marks (Data Protection Trustmark, APEC Cross-Border Privacy Rules, and APEC Privacy Recognition for Processors) in June 2021, only four years after setting up shop in the city-state (Alibaba Cloud, 2021). Table 1 shows that by 2024, both Alibaba and Tencent have displayed the full package, including International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) 27001, 27017, and 27018 standards for information security management, the Payment Card Industry Data Security Standard (PCI-DSS) Level 1 for payments, the Cloud Security Alliance Security, Trust & Assurance Registry (CSA STAR) certification for cloud security, and the Health Insurance Portability and Accountability Act (HIPAA) controls for health data—bringing them to parity with AWS on every audit ASEAN regulators routinely reference, bringing them to parity with AWS on every audit ASEAN regulators routinely reference. Because each badge is issued by an independent European or US assessor, the audits externalize trust: host officials need not take Beijing's word, only the regulator's.

Table 1. Comparative certifications of major cloud service providers in information security, privacy, and compliance (June 2025 data).

Certification category	AWS	Alibaba Cloud	Tencent Cloud	Standard origin	Governing body/authority
Information security	ISO/IEC 27001, 27017, 27018, and 27701	ISO/IEC 27001, 27017, 27018, 27701	ISO/ IEC 27001, 27017, 27018, 27701	Switzerland/ EU-led international collaboration	ISO (Geneva) and IEC
Privacy and data protection	General Data Protection Regulation(GDPR) and California Consumer Privacy Act(CCPA)	GDPR	GDPR	EU	European Data Protection Board
Financial services	PCI DSS Level 1, SOC 1/2/3	PCI DSS, SOC 1/2	PCI DSS, SOC 1/2	US-based global financial institutions	Payment Card Industry Security Standards Council (US) and American Institute of Certified Public Accountants (US)
Cloud security	CSA STAR Level 2	CSA STAR	CSA STAR	US-based global alliance	Cloud Security Alliance (US)
Industry-specific	Federal Risk and Authorization Management Program (FedRAMP), HIPAA, and MTCS	HIPAA and Multi-Tier Cloud Security (MTCS)	HIPAA and MTCS	US (HIPAA) and Singapore (MTCS)	US Department of Health and Infocomm Media Development Authority (IMDA) Singapore

Note: Data was compiled from corporate disclosures as of June 2025 and verified with certification authorities.

The breadth of that portfolio matters because the majority standard is Western in origin. Far from advancing a "China model," the firms prove they can inhabit the status quo ante more completely—and, crucially, more rapidly—than their US counterparts. Alibaba and Tencent attach sovereign plug-ins such as Singapore's MTCS Level-3 and OSPAR banking mark at launch, whereas AWS obtained MTCS earlier (in 2014) but added the financial-sector OSPAR mark only after it had already captured most regional workloads. Swift, full-stack adoption turns regulatory screening into a formality, demonstrating that controversial provenance need not predict divergent practice.

Compliance on paper becomes credible only when the servers themselves stay inside national borders. Alibaba opened its first overseas region and global cloud headquarters in Singapore in August 2015, then rolled out Kuala Lumpur (2017), Jakarta (2018), Bangkok (2022), and Ho Chi Minh City (2024), amassing nine availability

zones across the five study markets. Each launch embeds hyperscale hardware worth roughly $50 million (Swinhoe, 2023). Those nodes give regulators what the audits cannot: physical jurisdiction, inspection rights, and an emergency switch.

Tencent launched its first Indonesian data-center region in Jakarta in April 2021 and declared the facility fully operational the day it opened. The plant sits in the capital's central business district, runs dual utility feeds plus N+1 diesel capacity, and already hosts Bank Neo Commerce and JOOX streaming workloads (Swinhoe, 2021a). Tencent has since added second availability zones in Bangkok and pledged $500 million for a third Jakarta site by 2030 in collaboration with Telkomsel—a joint-venture structure that ties foreign capital to domestic political patrons (Swinhoe, 2021b).

Western incumbents, with first-mover advantages, act more slowly. AWS, Microsoft, and Google long served most ASEAN traffic from a 2010 Singapore hub; only in May 2024 did AWS announce a further $12 billion build-out through 2028 (Amazon, 2024). The contrast is not mere chronology but sequencing: Chinese firms saturate every major jurisdiction once they commit, pre-empting sovereignty objections, while US competitors add sovereign capacity reactively as market pressure intensifies.

Certifications externalize trust through third-party audits; bricks and mortar turn that symbolic assurance into an enforceable reality. Maintaining overlapping audits and sovereign-grade regions is costly, yet that very expense makes the signal credible: revocation would strand capital and invalidate certifications, aligning the providers' incentives with state demands. ASEAN governments reward the double lock with cloud-first procurement, national AI sandboxes, and flagship smart-city contracts, turning gatekeepers into stakeholders and demonstrating how spoke-states can weaponize interdependence from below.

Regulatory-infrastructure convergence, therefore, supplies the institutional "permission to operate" on which offshore embeddedness rests. It shows that when controversial-origin firms fully internalize the dominant rule system—procedurally and materially—they not only defuse geopolitical suspicion but also embed themselves so deeply that expulsion becomes costlier for host states than disciplined inclusion. The next section traces how Alibaba and Tencent leverage that granted legitimacy to assemble durable political-economic coalitions across Southeast Asia's fragmented data-governance landscape.

6.2. Network Integration via Stakeholder Coalitions

Controversial-origin cloud providers convert provisional regulatory approval into durable legitimacy by embedding themselves in host-country political and economic circuits. They form stakeholder coalitions—ministries, state-owned enterprises, and national-champion platforms—that acquire direct financial or reputational stakes in uninterrupted service provision, thereby transforming sovereignty anxieties into incentives for protection.

Indonesia furnishes a national-scale illustration. On 10 November 2024, GoTo Group, Tencent Cloud, and Alibaba Cloud concluded a tripartite pact—witnessed by President Prabowo Subianto—to expand domestic infrastructure and train Indonesian engineers ("Indonesia's GoTo, China's Tencent," 2024). Because GoTo underpins e-commerce, ride-hailing, and digital payments for millions of citizens, its dependence on Chinese clouds renders service continuity a quasi-public good; any disruption would entail immediate political costs

for the presidency and for GoTo's sovereign-wealth shareholders in Abu Dhabi and Singapore. Presidential endorsement thus elevates a commercial contract into a broad coalition linking executive authority, capital markets, and everyday users.

In Malaysia, the same outcome emerges through divergent templates. The Kuala Lumpur City Brain initiative, launched in 2018 by Alibaba Cloud and the Malaysia Digital Economy Corporation, required extensive algorithmic tailoring to local traffic regulations and infrastructural particularities (Farhan, 2018; Tan, 2018). The pilot phase reduced travel times by 12% (Azhar, 2019) while simultaneously developing Malaysian AI expertise and embedding Alibaba engineers in municipal routines. Tencent adopted a locally owned operator model: in August 2024, it partnered with Global Resources Management to create Alto Cloud, an internet-data-center campus in Cyberjaya that delivers more than 400 Tencent Cloud services through a Cloud Dedicated Zone architecture (Tencent Cloud, 2024). Because Malaysian capital retains equity control and front-end customer relationships, any sweeping restrictions on Tencent would inflict losses on domestic investors as well as the foreign entrant, dampening enthusiasm for exclusionary measures.

Vietnam underscores the value of coalition-based embedding under restrictive regulation. Alibaba leases capacity from Viettel and VNPT—state telcos that supply the bulk of national data-centre space—thereby situating foreign infrastructure within entities already entrusted with defence and public-security workloads (Nguyen, 2024). Tencent is negotiating a similar telecom-anchored entry. Embedding within incumbents that carry sovereign mandates provides an additional layer of political cover that greenfield builds would lack.

Western incumbents follow a different trajectory. AWS's $12 billion Singapore expansion and its $5 billion Jakarta investment are financed entirely from its Seattle headquarters, offering no equity shares to domestic state-owned enterprises (Amazon, 2024; Spencer, 2021). Microsoft's $2.2 billion Malaysia West region is likewise wholly owned, with local participation limited to skill memoranda of understanding (Microsoft, 2024). Even where AWS involves local firms, it relies on reseller tiers rather than joint-equity vehicles. This arm's-length posture contrasts with the equity joint ventures, smart-city pilots, and telecom co-location strategies that enable Chinese providers to cultivate mutual dependence.

Stakeholder coalitions thus reclassify Chinese clouds from potential political threats to development partners whose success is intertwined with influential domestic constituencies. Once ride-hailing dispatch, instant payment systems, or urban-mobility algorithms run on a Chinese platform, any interruption would impose immediate economic pain—and likely electoral repercussions—on host governments. The upfront costs borne by Alibaba and Tencent (e.g., seeding city Brain capabilities before revenue, accepting equity dilution, and pledging US$500 million for a third Jakarta availability zone) signal long-horizon commitment and solidify elite support. Network integration, therefore, deepens offshore embeddedness beyond rule compliance: audited certifications and onshore hardware secure the initial "permission to operate," while mutually dependent coalitions convert that permission into a political shield against future nationalist backlash.

6.3. Organizational Decoupling for Jurisdictional Assurance

Organizational decoupling secures host-state trust by embedding legal authority and day-to-day decision-making within the jurisdiction that grants market access. Rather than asking regulators to rely on

contractual promises, Chinese cloud providers create legally distinct regional units, whose boards, bank accounts, and compliance functions are governed by local law. This structural separation provides a concrete guarantee that Beijing cannot unilaterally override ASEAN statutes, completing the legitimation work begun by regulatory-infrastructure convergence and coalition building.

Alibaba Cloud pursues a headquarters-relocation model that recenters control in Singapore. In August 2015, the company registered Alibaba Cloud (Singapore) Pte Ltd as an independent holding company with its own directors and data-protection officers, thereby shifting oversight of all Southeast-Asian activities from Hangzhou to Singapore. Subsequent ventures, such as Indonesia's data-center cluster, which opened in February 2018, and the Fusionex partnership, which was signed in Malaysia in September 2017, report to this entity—not to the Chinese parent. By bringing corporate governance under Singaporean company law and the Personal Data Protection Act, Alibaba supplies regulators with a single, locally accountable node to which fines, audits, or suspension orders can be directed.

Tencent Cloud deploys a partner-anchored model that assigns contractual liability to domestic firms. In Thailand, the company signed a memorandum of understanding with Bangkok-listed systems integrator MFEC, stipulating that MFEC—not Tencent—acts as the counterparty for all public-sector and regulated-industry customers (MFEC, 2024). A parallel agreement in March 2025 designated state-affiliated Telkomsel as the front-end operator for a third Jakarta availability zone, while Tencent remains the platform licensor (Telkomsel, n.d.). These arrangements locate service-level guarantees, data-handling obligations, and tax reporting within entities answerable to Thai and Indonesian courts, leaving Tencent one step removed from coercive jurisdiction without relinquishing technical control.

ASEAN regulators value these structures because they convert abstract assurances into enforceable rights. Duplicate boards, autonomous compliance teams, and locally held assets allow officials to inspect shareholder registers, subpoena records, or revoke licenses without engaging Chinese authorities. Should geopolitical tensions escalate, ministries can compel the regional subsidiary or joint-venture partner to sever cross-border links or migrate sensitive workloads—actions that would be politically and technically costlier if the cloud were managed directly from China. Organizational decoupling thus realigns bargaining power, giving middle power states a credible "off switch" that is consistent with their sovereignty claims.

For Alibaba and Tencent, the additional administrative layers represent a calculated investment in political insurance. The expense of parallel governance structures is offset by access to government contracts, finance, healthcare, and other data-sensitive sectors that would remain out of reach without a demonstrable local accountability mechanism. By institutionalizing a locally enforceable chain of accountability, the providers turn what would otherwise be a unilateral compliance cost into a market differentiator, signaling to risk-averse corporate and public clients that their data will remain unequivocally subject to domestic law.

The absence of comparable measures among US and European competitors underscores that decoupling is a context-specific response to contested institutional origins rather than an industry-wide norm. Providers domiciled in GDPR or Cloud-Act jurisdictions already enjoy presumptive equivalence in ASEAN law; regulators address residual concerns through existing treaties and audit regimes rather than demanding local reincorporation. The contrast highlights why organizational decoupling is central to the offshore embeddedness of Chinese clouds: it addresses a credibility gap that arises only when the

provider's home legal system is treated as politically or juridically incompatible with the host state's data governance requirements.

7. Conclusion

This article challenges prevailing narratives of US–China technological competition by demonstrating how middle powers and non-state actors reshape data governance outcomes through strategic bargaining rather than passive alignment. The puzzle of Chinese cloud providers' success in ASEAN markets reveals that firms of controversial origin can convert institutional liabilities into competitive advantages, while middle powers exercise agency that transcends binary great power choices.

Offshore embeddedness explains this transformation through three complementary mechanisms. Regulatory-infrastructure convergence establishes technical credibility by exceeding Western competitors' compliance standards while embedding territorially fixed assets. Network integration via stakeholder coalitions manufactures domestic political protection by creating webs of mutual dependence among government ministries, state enterprises, and national platforms. Organizational decoupling provides jurisdictional assurance through locally accountable legal structures that give host governments enforceable control mechanisms. Together, these mechanisms enable firms of controversial origin to systematically convert data skepticism into managed market positions.

This framework advances understanding of technological competition in three ways. First, it reveals that firm legitimacy in contested domains depends less on home-country advantages than on strategic adaptation to host-state governance preferences. Chinese cloud providers have succeeded not by leveraging Beijing's network position but by demonstrating credible separation from it—challenging both international business assumptions about bridgeable institutional distance and weaponized interdependence theories treating firms as passive state conduits.

Second, the analysis exposes how middle powers exercise structural agency through sophisticated regulatory strategies. ASEAN governments do not merely choose between US and Chinese technological ecosystems; they actively recalibrate these choices by demanding simultaneous satisfaction of technical, political, and legal conditions. As gatekeeper-regulators, they control market entry through calibrated licensing; as infrastructure brokers, they convert regulatory consent into tangible national assets; and as coalition orchestrators, they embed foreign providers within domestic networks that align commercial success with development objectives.

Third, data governance frameworks function as leverage tools rather than defensive barriers. Rather than excluding controversial providers, sophisticated regulatory regimes enable selective inclusion on terms that maximize host-state benefits while minimizing sovereignty risks. This contradicts assumptions that middle powers must simply adapt to great power competition and demonstrates how they extract strategic value from technological rivalry.

The research illuminates the critical role of non-state actors in mediating competition outcomes. Chinese providers' success depends fundamentally on cultivating stakeholder coalitions in host countries with direct financial stakes in continued service provision. When ride-hailing platforms, payment systems, and smart

cities depend on Chinese infrastructure, disruption becomes politically costly regardless of geopolitical tensions. Indonesian President Prabowo's endorsement of the GoTo–Tencent–Alibaba partnership, Malaysia's integration of Alibaba's City Brain, and Vietnam's embedding of Chinese clouds within state telecoms all demonstrate how non-state stakeholders create constituencies for technological cooperation transcending formal government relations.

Future research should examine whether offshore embeddedness operates across different technological domains and regional contexts, track how intensifying competition affects middle power agency, and quantitatively analyze the marginal effects of individual mechanisms across institutional conditions.

The broader significance extends beyond Southeast Asia to challenge assumptions about technological competition in a multipolar world. Rather than bipolar division into competing technological spheres, we observe complex landscapes where middle powers leverage regulatory authority to extract benefits while maintaining flexibility, and Chinese firms succeed through offshore embedding within host data governance landscapes—operating beyond Beijing's direct control rather than implementing its preferences. This suggests future data and technology governance will be characterized by polycentric authority structures where middle powers and non-state actors exercise significant influence. Understanding these complex bargaining relationships, rather than focusing solely on great power competition, will be essential for predicting how critical technologies are governed. The politics of digital infrastructure are not predetermined by Washington or Beijing but emerge from strategic interactions across diverse stakeholders and contexts.

Acknowledgments

We are grateful for the constructive comments from external reviewers and from participants of the thematic issue workshop, which have substantially improved this article.

Funding

This research is supported by the Ministry of Education, Singapore, under its Academic Research Fund Tier 1 (RG50/23).

Conflict of Interests

The authors declare no conflict of interests.

LLMs Disclosure

We used OpenAI's ChatGPT-01 and Anthropic's Claude Sonnet 4 to assist with polishing the language in the final draft.

Supplementary Material

Supplementary material for this article is available online in the format provided by the authors (unedited).

References

Aglietta, M. (1979). *A theory of capitalist regulation: The U.S. experience*. Schocken Books.

Aguerre, C. (2024). Internet interoperability and polycentric attributes in global digital data ordering. In C. Aguerre, M. Campbell-Verduyn, & J. A. Scholte (Eds.), *Global digital data governance: Polycentric perspectives* (pp. 34–50). Routledge. https://doi.org/10.4324/9781003388418-4

Alibaba Cloud. (2021). *Alibaba Cloud secures all three data protection certifications in Singapore*. https://www.alibabacloud.com/en/press-room/alibaba-cloud-secure-all-three-data-protection-certifications-in-singapore

Amazon. (2024). *AWS deepens commitment to Singapore with additional S$12 billion investment by 2028 and new flagship AI programme*. https://www.aboutamazon.sg/news/aws/aws-deepens-commitment-to-singapore-with-additional-sg-12-billion-investment-by-2028-and-new-flagship-ai-programme

Arner, D. W., Castellano, G. G., & Selga, E. K. (2022). The transnational data governance problem. *Berkeley Technology Law Journal*, *37*, Article 623.

Azhar, K. (2019, October 30). Tech: Alibaba Cloud's City Brain could reduce KL travel time by 12%. *The Edge Malaysia*. https://www.theedgemarkets.com/article/tech-alibaba-clouds-city-brain-could-reduce-kl-travel-time-12

Beach, D., & Pedersen, R. B. (2019). *Process-tracing methods: Foundations and guidelines* (2nd ed.). University of Michigan Press.

Boyer, R. (2005). How and why capitalisms differ. *Economy and Society*, *34*(4), 509–557.

Broeders, D., Sukumar, A., Kello, M., & Andersen, L. H. (2025). Digital corporate autonomy: Geo-economics and corporate agency in conflict and competition. *Review of International Political Economy*, *32*(4), 1189–1213. https://doi.org/10.1080/09692290.2025.2468308

Chai, X. (2024, February 13). Alibaba Cloud has pressed the acceleration button for external expansion. *Moomoo*. https://www.moomoo.com/news/post/49172740/alibaba-cloud-has-pressed-the-acceleration-button-for-external-expansion?level=2&data_ticket=1753874376318849

Chander, A., & Lê, U. P. (2014). Data nationalism. *Emory Law Journal*, *64*, 677–739.

Chen, L., Li, Y., & Fan, D. (2018). How do emerging multinationals configure political connections across institutional contexts? *Global Strategy Journal*, *8*(3), 447–470. https://doi.org/10.1002/gsj.1187

Chen, X., & Gao, X. (2024). The regime complex for digital trade in Asia and China's engagement. *Asia Europe Journal*. Advance online publication. https://doi.org/10.1007/s10308-024-00705-0

Cheney, C. (2019). *China's Digital Silk Road: Strategic technological competition and exporting political illiberalism*. Council on Foreign Relations. https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political

Christophe, B., Giron, A., & Verin, G. (2023). A comparative analysis with machine learning of public data governance and AI policies in the European Union, United States, and China. *Journal of Intelligence Studies in Business*, *13*(2), 61–74.

Ciabuschi, F., Holm, U., & Martín, O. M. (2014). Dual embeddedness, influence and performance of innovating subsidiaries in the multinational corporation. *International Business Review*, *23*(5), 897–909. https://doi.org/10.1016/j.ibusrev.2014.02.002

Digital Trade and Data Governance Hub. (2024). *Global data governance mapping project*. https://globaldatagovernancemapping.org

Ding, J., & Dafoe, A. (2021). The logic of strategic assets: From oil to AI. *Security Studies*, *30*(2), 182–212. https://doi.org/10.1080/09636412.2021.1915583

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal*, *50*(1), 25–32.

Farhan. (2018, January 29). MDEC and DBKL partner with Alibaba to deploy traffic management AI platform. *Lowyat.NET*. https://www.lowyat.net/2018/153685/mdec-dbkl-partner-alibaba-deploy-traffic-management-ai-platform

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, *44*(1), 42–79.

Gao, X. (2022). An attractive alternative? China's approach to cyber governance and its implications for the Western model. *The International Spectator*, *57*(3), 15–30.

Gerring, J. (2007). *Case study research: Principles and practices*. Cambridge University Press.

Gjesvik, L. (2023). Digital choke-points and the limits of state power. *Survival*, *65*(2), 85–108.

Global Data Barometer. (2021). *Global Data Barometer: First edition*. https://firstedition.globaldatabarometer.org

Han, S. (2024). Data and statecraft: Why and how states localize data. *Business and Politics*, *26*(2), 263–288. https://doi.org/10.1017/bap.2023.41

He, Y. (2024). Chinese digital platform companies' expansion in the Belt and Road countries. *The Information Society*, *40*(2), 96–119. https://doi.org/10.1080/01972243.2024.2317058

Herbert Smith Freehills. (2024). *Thailand's new legislation on cross-border transfer of personal data*. https://www.herbertsmithfreehills.com/notes/data/2024-01/thailands-new-legislation-on-cross-border-transfer-of-personal-data

Indonesia's GoTo, China's Tencent, Alibaba agree on cloud infrastructure development. (2024, November 10). *The Business Times*. https://www.businesstimes.com.sg/international/asean/indonesias-goto-chinas-tencent-alibaba-agree-cloud-infrastructure-development

Kausche, K., & Weiss, M. (2024). Platform power and regulatory capture in digital governance. *Business and Politics*, *27*(2), 284–308. https://doi.org/10.1017/bap.2024.33

Kostova, T., & Zaheer, S. (1999). Organizational legitimacy under conditions of complexity: The case of the multinational enterprise. *Academy of Management Review*, *24*(1), 64–81.

Lehdonvirta, V., Wú, B., & Hawkins, Z. (2025). Weaponised interdependence in a bipolar world: How economic forces and security interests shape the global reach of US and Chinese cloud data centres. *Review of International Political Economy*. Advance online publication. https://doi.org/10.1080/09692290.2025.2489077

Li, J., Meyer, K. E., Zhang, H., & Ding, Y. (2018). Diplomatic and corporate networks: Bridges to foreign locations. *Journal of International Business Studies*, *49*(6), 659–683.

Lipietz, A. (1987). *Mirages and miracles: The crises of global Fordism*. Verso.

McGinnis, M. D. (2011). An introduction to IAD and the language of the Ostrom workshop: A simple guide to a complex framework. *Policy Studies Journal*, *39*(1), 169–183.

MFEC. (2024). *MFEC signed MoU with Tencent Cloud to drive technological innovation in Thailand and globally*. https://www.mfec.co.th/en/success-stories/mfec-mou-tencent-cloud

Microsoft. (2024). *Microsoft announces US$2.2 billion investment to fuel Malaysia's cloud and AI transformation*. https://news.microsoft.com/apac/2024/05/02/microsoft-announces-us2-2-billion-investment-to-fuel-malaysias-cloud-and-ai-transformation

Minister calls for protection of Indonesia's digital sovereignty. (2022, August 17). *Antara*. https://en.antaranews.com/news/246946/minister-calls-for-protection-of-indonesias-digital-sovereignty

Minister for Communications and Information. (2021). *Personal data protection (notification of data breaches) regulations 2021*. Singapore Statutes Online. https://sso.agc.gov.sg/SL/PDPA2012-S64-2021

Ministry of Communications and Digital. (2021). *Malaysia digital economy blueprint (MyDIGITAL)*. Government of Malaysia.

Muellner, J., Klopf, P., & Nell, P. C. (2017). Trojan horses or local allies: Host-country national managers in developing-market subsidiaries. *Journal of International Management*, *23*(3), 306–325. https://doi.org/10.1016/j.intman.2016.12.001

Nguyen, K. (2024, May 2). Alibaba plans $1 billion data centre in Vietnam. *Vietnam Investment Review*. https://vir.com.vn/alibaba-plans-1-billion-data-centre-in-vietnam-110812.html

Oh, Y. A., & No, S. (2020). The patterns of state-firm coordination in China's private sector internationalization: China's mergers and acquisitions in Southeast Asia. *The Pacific Review*, *33*(6), 873–899.

Ostrom, E. (2010). Beyond markets and states: Polycentric governance of complex economic systems. *American Economic Review*, *100*(3), 641–672.

Pearson, M. M., Rithmire, M., & Tsai, K. S. (2022). China's party-state capitalism and international backlash: From interdependence to insecurity. *International Security*, *47*(2), 135–176.

Ragin, C. C. (2014). *The comparative method: Moving beyond qualitative and quantitative strategies*. University of California Press.

Rithmire, M., & Han, C. (2021). *The clean network and the future of global technology* competition. Harvard Business School Case.

Shen, H. (2018). Building a Digital Silk Road? Situating the internet in China's Belt and Road Initiative. *International Journal of Communication*, *12*, 2683–2701.

Spencer, L. (2021, December 13). AWS launches Indonesia cloud region, pledges $5B investment. *Channel Asia*. https://www.channelasia.tech/article/1266775/aws-launches-indonesia-cloud-region-pledges-5b-investment.html

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review*, *20*(3), 571–610.

Sun, P., Mellahi, K., & Wright, M. (2012). The contingent value of corporate political ties. *Academy of Management Perspectives*, *26*(3), 35–52. https://doi.org/10.5465/amp.2011.0164

Suruga, T. (2023, November 15). Southeast Asia's digital battle: Chinese and U.S. big tech face off over $1tn market. *Nikkei Asia*. https://asia.nikkei.com/Spotlight/The-Big-Story/Southeast-Asia-s-digital-battle-Chinese-and-U.S.-Big-Tech-face-off-over-1tn-market

Swinhoe, D. (2021a, April 12). Tencent Cloud launches first data center in Jakarta, Indonesia. *Data Centre Dynamics*. https://www.datacenterdynamics.com/en/news/tencent-cloud-launches-first-data-center-in-jakarta-indonesia

Swinhoe, D. (2021b, June 3). Tencent opens four new availability zones in Asia and Europe. *Data Centre Dynamics*. https://www.datacenterdynamics.com/en/news/tencent-opens-four-new-availability-zones-in-asia-and-europe

Swinhoe, D. (2023, October 11). NTT launches data center in Cyberjaya, Malaysia. *Data Centre Dynamics*. https://www.datacenterdynamics.com/en/news/ntt-launches-data-center-in-cyberjaya-malaysia

Tan, D. (2018). *Alibaba brings 'City Brain' traffic control system to KL*. Paul Tan. https://paultan.org/2018/01/30/alibaba-to-set-up-ai-traffic-control-system-for-kl-traffic

Tang, M. (2020). Huawei versus the United States? The geopolitics of exterritorial internet infrastructure. *International Journal of Communication*, *14*, 4556–4577.

Telkomsel. (n.d.). *Telkomsel and Tencent Cloud develop AI and cloud solutions to enhance customer experience*. https://www.telkomsel.com/en/about-us/news/telkomsel-and-tencent-cloud-develop-ai-and-cloud-solutions-enhance-customer

Tencent Cloud. (2024). *Alto Cloud grand launching 2024—Powered by Tencent Cloud, Alto Cloud joins the Malaysian market as a full-service cloud solutions provider*. https://www.tencentcloud.com/dynamic/news-details/100594

The Government of Vietnam. (2022). *Elaborating a number of articles of the law on cybersecurity of Vietnam* (Decree No. 53/2022/ND-CP). https://thuvienphapluat.vn/van-ban/EN/Cong-nghe-thong-tin/Decree-53-2022-ND-CP-elaborating-the-Law-on-cybersecurity-of-Vietnam/527750/tieng-anh.aspx

Xu, D., & Shenkar, O. (2002). Institutional distance and the multinational enterprise. *Academy of Management Review*, *27*(4), 608–618.

Xu, K. (2023). *US vs China: A cloud proxy war*. Interconnected. https://interconnected.blog/us-vs-china-a-cloud-proxy-war

Yin, R. K. (2018). *Case study research: Design and methods* (6th ed.). Sage.

Zaheer, S. (1995). Overcoming the liability of foreignness. *Academy of Management Journal*, *38*(2), 341–363.

About the Authors

Binyi Yang is a PhD candidate at the S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore. Her research explores state-business relationships in China's technological development, with a focus on clean-tech sectors, subnational dynamics, and the global expansion strategies of Chinese firms.

Mingjiang Li is an associate professor and Provost's Chair in international relations at S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. His main research interests include Chinese foreign policy, China–ASEAN relations, Sino–US relations, and Asia-Pacific security.