



EPIC-PP-2026-009 · RESEARCH ARTICLE · GULF STRATEGY

Data Sovereignty Without Borders: Gulf States and the Geopolitics of AI Compute

EPIC – Emirati Perspectives and Insight Centre

Seeing what others miss...

20 October 2026

CC BY 4.0 · Creative Commons Attribution 4.0 International · creativecommons.org/licenses/by/4.0

Data Sovereignty Without Borders: Gulf States and the Geopolitics of AI Compute

EPIC – EMIRATI PERSPECTIVES AND INSIGHT CENTRE

EPIC-PP-2026-009 · Gulf Strategy · Published 20 October 2026

© 2026 EPIC – Emirati Perspectives and Insight Centre. Released under Creative Commons Attribution 4.0 International (CC BY 4.0): <https://creativecommons.org/licenses/by/4.0/>

EPIC is an independent research initiative in formation. It is not yet a registered or licensed entity. EPIC does not accept donations, payments or contracts.

Abstract

Gulf states are racing to host artificial intelligence (AI) compute on their own soil while remaining deeply dependent on foreign chips, cloud platforms, and export-control regimes. This study examines that paradox as a strategic problem for Bahrain and the wider Gulf Cooperation Council (GCC). Drawing on official strategy documents, primary corporate announcements, national data-protection statutes, and the international-relations literature on digital sovereignty and weaponized interdependence, the paper argues that Gulf "sovereign AI" is better understood as negotiated interdependence than as autarky. Local data centres, Arabic-language models, and personal-data laws create meaningful jurisdictional control over where workloads run and how personal data travel. They do not, however, eliminate dependence on United States (US) advanced semiconductors or on hyperscale software ecosystems. Bahrain's cloud-computing framework for foreign parties and its 2025 national AI policy illustrate a smaller-state pathway: legal hosting, regulatory alignment, and GCC ethical coordination rather than gigawatt-scale campus competition. The paper concludes with policy implications for compute diplomacy, cross-border data rules, and regional cooperation that treat sovereignty as layered control rather than territorial self-sufficiency.

Keywords: *data sovereignty; AI compute; Gulf Cooperation Council; Bahrain; export controls; cloud governance*

1. Introduction

In May 2025, Saudi Arabia's Public Investment Fund announced HUMAIN, a PIF-owned company charged with operating across the artificial intelligence (AI) value chain, from data centres and cloud capacity to advanced models, including a multimodal Arabic large language model (Public Investment Fund [PIF], 2025). Months earlier, in April 2024, Microsoft had announced a USD 1.5 billion strategic investment in Abu Dhabi-based G42, with Microsoft's vice chair joining the G42 board and both firms committing to an Intergovernmental Assurance Agreement developed in consultation with the governments of the United Arab Emirates (UAE) and the United States (Microsoft, 2024). Parallel to these corporate moves, Bahrain's Information and eGovernment Authority launched, in July 2025, a national policy for the use of AI in government and formally adopted a GCC guiding manual on AI ethics (Information & eGovernment Authority [iGA], 2025). Taken together, these developments signal that the Gulf is no longer only a consumer of AI services hosted elsewhere. It is becoming a contested site of AI compute—the physical and organisational capacity to train, fine-tune, and serve large models.

Yet the politics of that capacity cannot be reduced to megawatts on desert plots. Advanced GPUs remain subject to US export-control regimes; hyperscale software stacks remain concentrated among a handful of firms; and personal-data laws across the GCC create uneven rules for cross-border transfer. The result is a sovereignty that is territorially ambitious and structurally incomplete. This paper names that condition data sovereignty without borders: the pursuit of jurisdictional control over data and compute in a technological order whose critical inputs—chips, fabrication, foundational model weights, and cloud orchestration—routinely cross borders and remain subject to foreign law and foreign firms.

The argument is strategic rather than purely legal. Drawing on Farrell and Newman's (2019) account of weaponised interdependence, and on the growing literature on digital sovereignty, the paper treats Gulf compute strategy as an attempt to occupy advantageous nodes in networks that can also be used coercively. Local hosting and national AI champions raise the cost of exclusion and create bargaining chips. They do not abolish asymmetric dependence. For Bahrain and other smaller GCC states, the implication is not to mimic the largest campus projects, but to specialise in legal hosting, trusted interconnection, and regional governance that convert interdependence into influence.

The study proceeds as follows. Section 2 situates the analysis in the literatures on digital sovereignty and interdependence. Section 3 maps the Gulf's compute build-out and national AI strategies, relying on primary announcements rather than secondary capacity estimates where those estimates conflict. Section 4 examines the legal layer: personal-data regimes, Bahrain's cloud and data-embassy framework, and free-zone rules such as the Dubai International Financial Centre's Regulation 10 on autonomous systems. Section 5 develops the paradox of sovereignty without borders and its implications for Bahrain. Section 6 offers policy recommendations. Section 7 concludes.

Methodologically, this is a qualitative strategic study. It triangulates primary institutional texts (statutes, official strategies, and corporate press materials issued by the organisations themselves) with established theoretical work on interdependence and digital sovereignty. It does not claim ethnographic access to confidential assurance schedules or to non-public capacity ledgers. Where public secondary reporting offers precise megawatt or chip-quantity figures that cannot be confirmed in primary documents consulted for this study, those figures are omitted or flagged as unverified. The payoff of that restraint is reliability: every concrete institutional claim below is meant to be checkable.

The contribution is threefold. First, it reframes Gulf 'sovereign AI' as negotiated interdependence, clarifying what local compute can and cannot purchase. Second, it places Bahrain's legal-hosting model in comparative Gulf perspective, arguing that small-state sovereignty strategies can centre jurisdictional design. Third, it translates that analysis into policy instruments—layered metrics, compute diplomacy, multi-homing, and shared Arabic evaluation public goods—that follow from the diagnosis rather than from generic AI ethics checklists.

2. Conceptual Frame: Digital Sovereignty and Weaponised Interdependence

2.1 Digital Sovereignty as Layered Control

Empirically, layered control helps explain why Gulf governments can simultaneously deepen ties with US cloud providers and tighten domestic data rules. The apparent contradiction dissolves once sovereignty is disaggregated. Hosting a model endpoint in Abu Dhabi or Riyadh strengthens territorial and organisational control even if the accelerator inside the rack remains subject to a US licence condition. Conversely, a strictly extraterritorial SaaS arrangement may leave personal-data controllers exposed under local PDPL-type statutes even when no rack sits onshore. Policy debate that collapses these layers into a single slogan of 'sovereign AI' obscures trade-offs that procurement officers already face in practice.

The European debate is instructive as a foil rather than a template. European digital-sovereignty initiatives have often emphasised regulatory power over large platforms and industrial policy for cloud and chips. Gulf initiatives emphasise capital deployment and bilateral assurance with the technology frontier. Both respond to dependence; they choose different instruments. For Bahrain, the European analogy is useful mainly in reminding policymakers that law can be a sovereignty tool—an insight already embedded in the 2018 cloud law—without requiring Bahrain to replicate EU market scale.

Digital sovereignty has become a travelling concept rather than a settled doctrine. Pohle and Thiel (2020) describe it as a political claim to authoritative control over digital infrastructures, data flows, and the norms that govern them, advanced by states that fear dependence on foreign platforms. The term spans very different projects: European efforts to regulate platforms and foster industrial alternatives; Chinese state-centric control

of networks and data; and, more recently, Gulf programmes that pair sovereign wealth with partnerships with US technology firms. What these projects share is less autarky than a demand for leverage—over storage location, access rights, auditability, and the conditions under which foreign technology may be used for public functions.

For the purposes of this paper, data sovereignty is treated as layered control along at least four axes: (1) territorial hosting of storage and compute; (2) legal authority over personal and state data, including transfer restrictions; (3) organisational ownership or governance of AI firms and cloud regions; and (4) technological capacity to train or adapt models for local languages and sectors. A state may score highly on one axis and poorly on another. Gulf strategies currently emphasise axes (1)–(3) and invest heavily in axis (4) through Arabic-language models, while remaining constrained on the semiconductor manufacturing and advanced-chip design layers that sit upstream of all four.

2.2 Weaponised Interdependence and Compute

Export-control instruments make the chokepoint concrete. The US Bureau of Industry and Security's (BIS, 2023) October 2023 Federal Register rule expanding controls on advanced computing items and supercomputer end uses is part of a wider effort to restrict diffusion of high-end AI training capacity to destinations of concern. Gulf states are not the primary stated targets of China-focused controls, yet they sit inside a licensing environment in which advanced accelerators are no longer ordinary dual-use commodities. Access becomes a negotiated privilege, often bundled with security assurances, reporting duties, and limits on onward transfer or on the involvement of restricted parties.

Weaponisation need not mean constant coercion. Farrell and Newman emphasise potential power embedded in network position. The day-to-day experience of Gulf AI firms may be commercial partnership rather than denial. The strategic point is residual vulnerability: a change in US licensing policy, or a political shock that reopens assurance terms, can reprice or reschedule capacity. Domestic data centres cannot fully hedge that risk; they can only reduce certain secondary risks, such as latency and some forms of foreign law-enforcement access to stored personal data.

Farrell and Newman (2019) argue that asymmetric networks enable states that occupy chokepoints to weaponise interdependence through the panopticon effect (surveillance of network traffic) and the chokepoint effect (denial of access). Global semiconductor supply chains and cloud platforms exhibit both features. Advanced AI accelerators are designed primarily by US firms and fabricated through tightly concentrated manufacturing ecosystems. Export licensing therefore becomes a strategic instrument: access to high-performance chips for training frontier models is not a pure market transaction but a politically mediated privilege.

The Gulf case fits this framework with an important twist. Gulf states are capital-rich demand nodes seeking to host capacity, not manufacturing hubs seeking to displace TSMC or Nvidia. Their strategy is to become indispensable regional platforms—for Arabic-language AI, for energy-adjacent compute, and for cloud services serving neighbouring markets—while negotiating privileged access to controlled chips through government-to-government and firm-to-firm assurance arrangements. Microsoft's 2024 investment in G42 (Microsoft, 2024) explicitly linked commercial partnership to an Intergovernmental Assurance Agreement and to compliance with US and international trade and security rules. Sovereignty here is performed through compliance architecture as much as through territorial ownership.

2.3 Why Borders Still Matter—and Why They Do Not Suffice

Borders still matter because data-protection law, criminal process, and national-security classification attach to jurisdiction. A model fine-tuned on health records in Riyadh is not legally interchangeable with the same technical process in a foreign region if transfer rules forbid or condition the export of personal data. Borders do not suffice, however, because model weights, prompts, and embeddings can move even when raw datasets stay put; because administrators with privileged credentials may sit abroad; and because the chips themselves may be

recalled, denied upgrades, or subjected to use restrictions by the exporting state. Data sovereignty without borders is therefore not a slogan of borderlessness. It is a description of sovereignty that must be exercised through and despite cross-border technological dependence.

3. The Gulf Compute Landscape: Strategies, Champions, and Asymmetries

3.1 National Strategies and Institutional Anchors

Institutional anchors matter because compute projects outlast press cycles. SDAIA's dual role in data governance and AI strategy in Saudi Arabia creates a single bureaucratic centre of gravity for PDPL enforcement and national AI ambition. The UAE's early creation of a dedicated AI ministerial portfolio and subsequent institutional updates similarly signalled that AI was not a side project of a telecoms regulator alone. Bahrain's iGA-led 2025 policy, issued under the Ministerial Committee for Information Technology and Communication, places government AI use inside the digital-government apparatus and ties it explicitly to the PDPL, state-documents protection, and open-data policy. The bureaucratic home of AI policy shapes whether compute is treated as industrial policy, security policy, or public-sector modernisation—or, as is increasingly the case, all three.

Soft-law density should not be mistaken for legal vacuum. Ethics manuals and strategies create organisational expectations, training budgets, and procurement checklists even when courts cannot yet enforce an 'AI Act.' They also create regional reference points. Bahrain's adoption of the GCC ethics manual is a coordination move: it imports shared language on human autonomy, safety, justice and non-discrimination, privacy, and data security, while leaving hard infrastructure competition untouched. Normative convergence with infrastructural rivalry is a recognisable GCC pattern in other sectors; AI is reproducing it.

The UAE's National Strategy for Artificial Intelligence 2031 (United Arab Emirates, n.d.) set an early regional marker by framing AI as a whole-of-government and economic project, with ambitions spanning sector deployment, talent, research, data infrastructure, and governance. Saudi Arabia institutionalised a parallel ambition through the Saudi Data and AI Authority (SDAIA) under Vision 2030, positioning the Kingdom as a data and AI hub under Vision 2030. Bahrain's path has been more incremental: a personal-data protection law in 2018, a cloud-computing law creating a distinctive hosting regime the same year, and, in 2025, a government-sector National Policy for the Use of Artificial Intelligence together with adoption of a GCC AI ethics manual. Qatar has long operated under Law No. 13 of 2016 on personal data privacy protection and a 2019 national AI strategy framing, while Kuwait has relied more heavily on sectoral regulation, including Communications and Information Technology Regulatory Authority rules on data privacy for licensed providers.

These instruments differ in legal force. A reading of the statutes and policies cited here indicates that comprehensive personal-data statutes now exist in most GCC states, but binding, general AI statutes remain scarce; strategies and ethics manuals are largely soft law. That asymmetry matters for compute geopolitics. Soft-law AI ethics can travel quickly across the GCC, as Bahrain's adoption of the regional ethics manual shows. Hard constraints on chips and cloud regions travel through export licences and commercial contracts.

3.2 Corporate Champions and Partnership Architectures

The G42–Microsoft structure is notable for its explicit dual-government framing. The public announcement presents not only equity and go-to-market arrangements but also a first-of-its-kind Intergovernmental Assurance Agreement and a commitment to world-leading standards in AI safety and security, developed with UAE and US government consultation. Whatever the confidential schedules of that agreement contain, the public form already teaches a lesson: in the current geopolitical market for AI, large Gulf partnerships advertise compliance architecture as a feature. Trust is staged for multiple audiences—domestic publics, US regulators, and third-country customers.

HUMAIN's public launch materials emphasise unified operation across the value chain and Arabic multimodal capability under PIF ownership. That ownership structure simplifies principal-agent alignment relative to a publicly traded hyperscaler, but it also concentrates project risk on the sovereign balance sheet. The strategic wager is that vertical integration will accelerate domestic capacity and intellectual property. The open question—which this paper cannot settle from public sources alone—is how far vertical integration can proceed before it re-encounters the same upstream chip and fabrication constraints that face every other national AI project outside the manufacturing core.

Secondary reporting has described multi-gigawatt ambitions, multi-vendor GPU procurement, and large construction contracts on both sides of the UAE–Saudi competition. This study deliberately refrains from treating unverified megawatt totals as established fact. What matters analytically is not the precise peak-megawatt claim of any given week, but the direction of travel: sovereign capital is being used to pull training and inference capacity onto Gulf territory under national champions, while the silicon and much of the software stack remain foreign.

Two partnership architectures currently dominate the upper Gulf. The UAE model, exemplified by G42, combines a national AI conglomerate with deep hyperscaler alignment. Microsoft's April 2024 announcement (Microsoft, 2024) stated a USD 1.5 billion investment, a board seat for Brad Smith, a commitment that G42 would run AI applications on Microsoft Azure, a planned USD 1 billion developer fund, and the Intergovernmental Assurance Agreement noted above. Subsequent Microsoft communications in 2025 described a further major UAE investment package and a 200-megawatt datacentre expansion delivered through Khazna Data Centers, a G42 subsidiary, expected to begin coming online before the end of 2026 (Microsoft, 2025). The partnership narrative emphasises sovereign cloud services alongside global collaboration—an explicit coupling of local control language with foreign platform dependence.

The Saudi model, exemplified by HUMAIN, is framed as a vertically integrated, PIF-owned operating company spanning infrastructure, cloud, models, and applications. The 12 May 2025 PIF (2025) press release presents HUMAIN as consolidating data-centre initiatives, procuring hardware, and offering advanced Arabic multimodal models, while contributing to the Kingdom's positioning as a competitive AI hub. Public reporting has since described multi-vendor hardware strategies and large construction contracts; where such secondary figures conflict or cannot be confirmed from primary filings in this study, they are treated cautiously. What can be stated securely from the PIF announcement is institutional intent: sovereign ownership of an AI operating company that seeks to span the stack, not merely to buy cloud credits.

These architectures are competitive and complementary at once. Both seek regional hub status; both remain dependent on US-origin accelerators; both invest in Arabic-language capability as a differentiating asset. For smaller GCC states, the strategic question is less which giant to imitate than how to interconnect with both while preserving legal autonomy and bargaining room.

3.3 Energy, Geography, and the Materiality of Compute

Water and cooling deserve equal billing with electricity in any honest Gulf compute debate. Even where electricity is abundant, high-density AI racks impose cooling designs with environmental and planning externalities. Coastal sites, district cooling, and emerging liquid-cooling designs will shape which projects are socially and environmentally sustainable. A sovereignty strategy that ignores these material constraints will overstate feasible scale. Bahrain's smaller land and water envelope is a reason to prefer high-value, lower-sprawl hosting and interconnection functions over maximal training campuses.

Submarine cables and terrestrial routes are the quiet infrastructure of data sovereignty. Control over landing stations, diversity of routes, and repair arrangements affects whether 'local' compute remains reachable during regional disruption. States that invest in compute without investing in resilient connectivity risk building expensive islands. Here again, Bahrain's historic role as a financial and communications node is an asset if maintained.

AI training clusters are energy- and cooling-intensive. Gulf states advertise abundant energy, available land, and submarine-cable connectivity between Asia, Africa, and Europe as locational advantages. Those advantages are real but not unique; they are shared, in different mixes, with other aspiring hubs. What is more distinctive is the combination of sovereign capital, relatively centralised decision-making, and a willingness to negotiate security assurances with Washington in exchange for chip access. Material geography enables the pitch; political economy closes the deal.

4. The Legal Layer: Personal Data, Cloud Hosting, and Free-Zone AI Rules

4.1 Personal-Data Regimes across the GCC

Cross-border transfer rules are the hinge between data protection and compute location. Where transfers require adequacy findings, contractual clauses, or authority approval, public-sector and regulated private-sector entities face strong incentives to prefer in-country processing for personal data. AI systems that embed personal data in prompts, retrieval corpora, or fine-tuning sets inherit those incentives. The unsettled question across several GCC jurisdictions is how embeddings, logs, and model-generated outputs that may re-identify individuals will be classified. Until regulators issue clearer AI-specific guidance, conservative counsel will often recommend onshore processing for sensitive workloads—an outcome that supports local cloud regions even without an explicit data-localisation statute.

Fragmentation has costs. A bank operating in four GCC markets may face four documentation regimes for the same AI credit tool. That cost can slow beneficial deployment and also push firms toward the freest or most familiar free-zone rule-set, which may not be the rule-set most protective of data subjects. Regional mutual recognition for defined low-risk processing, paired with stricter scrutiny for high-risk automated decision-making, would better match risk to compliance burden.

Saudi Arabia's Personal Data Protection Law (PDPL), issued under Royal Decree M/19 (Saudi Data and AI Authority [SDAIA], 2023) and administered with SDAIA as competent authority, applies to processing inside the Kingdom and, in specified circumstances, to processing of residents' data from abroad. Implementing and transfer regulations condition cross-border flows. The UAE's Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (United Arab Emirates, 2021) establishes a federal framework, complemented by free-zone regimes in the Dubai International Financial Centre (DIFC) and Abu Dhabi Global Market (ADGM). Bahrain's Law No. 30 of 2018 on personal data protection (Kingdom of Bahrain, 2018a) created an early GCC comprehensive statute, later elaborated through ministerial decisions on transfers and controller duties. Qatar's Law No. 13 of 2016 (State of Qatar, 2016) remains a foundational privacy statute. Kuwait's framework has been more sectoral, with the Communications and Information Technology Regulatory Authority issuing data-privacy regulation applicable to licensed communications and information-technology providers.

None of these laws is an AI Act. They regulate personal data that AI systems process. Their strategic effect on compute is nevertheless substantial: they raise the value of in-country or in-region cloud regions for government and regulated-industry workloads, and they create compliance demand for contractual clauses, transfer impact assessments, and local storage. Sovereignty claims are partly exercised as data-protection compliance.

4.2 Bahrain's Cloud Law and the Data-Embassy Concept

Comparisons with European 'data embassy' experiments and with diplomatic-premises analogies should be handled carefully. Bahrain's statute is a domestic cloud-services law with a choice-of-law and judicial-competence design for foreign-customer data in designated facilities; it is not a Vienna Convention diplomatic mission. The policy innovation is nonetheless significant for a small state: instead of only demanding that data stay inside Bahrain, Bahrain also offers to host foreign sovereign or enterprise data under the foreign principal's law. That is an export of trust rather than an import of isolation.

Operational success depends on credible separation: physical security, identity and access management, logging, and processes for handling conflicting orders. If foreign courts and Bahraini authorities issue incompatible demands, the notification and escalation pathways must be clear. Transparency about those pathways—within the limits of security—would strengthen the product. Opacity would invite suspicion that the embassy metaphor oversells the legal firewall.

Bahrain's Decree-Law No. 56 of 2018 on providing cloud computing services to foreign parties is regionally distinctive (Kingdom of Bahrain, 2018b). Section 3 provides that customer content held in designated data centres for foreign parties is subject to the exclusive jurisdiction of the courts, public authorities, and laws of the foreign state in which the customer is established, including orders for access, disclosure, preservation, or integrity of that content; a service provider receiving such an order must inform Bahrain's Attorney General in writing. Foreign states and data centres are designated by Council of Ministers regulation. Secondary legal commentary commonly describes this as a 'data embassy' or extraterritorial hosting arrangement: physical infrastructure in Bahrain, legal regime partly of the foreign principal. Whether one accepts the embassy metaphor or not, the design is clear. Bahrain offers itself as a trusted host whose value proposition is legal interoperability, not only cheap power.

For a small island economy, that design is strategically coherent. Bahrain is unlikely to outbuild Saudi or UAE training campuses on raw scale. It can, however, specialise in jurisdictional products: cloud regions attractive to foreign governments and firms that want Middle East latency with familiar legal process; interconnection between larger Gulf compute pools; and regulatory credibility reinforced by the 2018 PDPL and the 2025 government AI policy. Data sovereignty without borders, in the Bahraini variant, means inviting borders—foreign legal borders—into domestic data centres under controlled conditions.

4.3 Free-Zone Soft Law and Harder Edges: DIFC Regulation 10

Inside the DIFC, Regulation 10 on personal data processed through autonomous and semi-autonomous systems, in force from 1 September 2023 (Dubai International Financial Centre [DIFC], 2023), addresses personal data processed through autonomous and semi-autonomous systems. It is among the few binding AI-adjacent rules in the region and imposes documentation, transparency, and accountability duties on operators within that free zone. Its geographic scope is limited, but its demonstration effect is not. It shows that Gulf jurisdictions can move from strategy documents to enforceable process requirements for automated systems, at least in internationally oriented financial free zones. For compute geopolitics, free-zone rules matter because much cross-border cloud contracting for regional finance already routes through such jurisdictions.

5. Sovereignty Without Borders: The Strategic Paradox

5.1 What Local Compute Actually Buys

A further benefit is narrative and deterrent. Announcing domestic capacity signals modernity to investors and citizens and may deter casual data demands by foreign commercial counterparties who find it easier to insist on home-jurisdiction processing when no local alternative exists. In procurement negotiations with global vendors, a credible national alternative—even if only partial—can improve contract terms on audit rights, data residency, and exit assistance. These are classic gains from creating a BATNA (best alternative to a negotiated agreement) in technology markets.

The corresponding risk is capability theatre: measuring success by announced partnerships and renderings of campuses rather than by uptime, utilisation, evaluated model quality, and auditable compliance. Strategic communication is part of statecraft; it becomes a vulnerability when it outruns engineering reality. Layered metrics, proposed below, are a partial antidote.

Local compute buys latency, resiliency for some failure modes, political symbolism, and a stronger hand in procurement negotiations. It also buys a more credible claim that sensitive workloads remain subject to domestic courts and regulators. For Arabic-language public services, local or regional fine-tuning capacity can improve performance and reduce the need to ship domain data abroad. These are not trivial gains. They convert abstract sovereignty talk into operational options.

Local compute does not buy independence from export licences for advanced accelerators. It does not buy an indigenous lithography stack. It does not automatically buy control over closed-source model updates pushed by foreign vendors. And it does not dissolve the possibility that assurance agreements with exporting states will condition who may access systems, how models may be trained, and which third-country entities must be excluded. The Microsoft–G42 public materials (Microsoft, 2024) are unusually frank on this point: the partnership is framed as compliant with US and international trade and security rules, not as an escape from them.

5.2 Negotiated Interdependence as Strategy

Once those limits are acknowledged, Gulf policy looks less like failed autarky and more like deliberate negotiated interdependence. States offer capital, energy, land, and geopolitical alignment; technology providers and exporting states offer chips, platforms, and market access; both sides write assurance architectures. Farrell and Newman's chokepoint logic predicts that the chip-exporting state retains coercive potential. The Gulf countermove is to raise the commercial and political cost of coercion by becoming a large, organised demand node and a regional distribution hub for AI services into adjacent markets. Dependence remains, but it becomes mutualised.

This reading disciplines both hype and despair. Hype that equates a domestic data centre with digital independence misunderstands the stack. Despair that treats every foreign chip as nullifying sovereignty misunderstands law and organisation: jurisdiction over data, personnel clearance, audit rights, and procurement rules are real instruments even when silicon is imported.

5.3 Regional Fragmentation Risks

Labour-market and skills fragmentation compounds infrastructure fragmentation. If each national champion builds closed training pipelines and proprietary evaluation harnesses, Arabic AI research will duplicate scarce expertise. A GCC shared research cloud for universities—distinct from classified government compute—could mitigate that risk. Bahrain's universities and regulatory agencies could host convening functions even if the heaviest training runs elsewhere.

A second paradox follows. As Saudi Arabia and the UAE scale national champions, smaller states face a choice between hitching to one ecosystem and maintaining multi-homing. Multi-homing preserves bargaining power but raises integration costs. Exclusive hitching lowers costs but deepens a single point of political and technical failure. GCC-level ethics guidance, such as the manual Bahrain adopted in 2025, softens normative divergence without resolving infrastructure competition. Without deliberate interconnection standards—for identity, logging, incident response, and cross-border government data sharing—the region could reproduce, inside the Gulf, the very fragmentation that digital-sovereignty projects were meant to escape.

5.4 Bahrain's Niche in a Two-Speed Region

Bahrain's comparative advantage lies in trust services rather than raw training capacity. The cloud law's foreign-law hosting mechanism, the PDPL, the government AI policy's four pillars (legal compliance, adoption, awareness, and cooperation), and long-standing financial-sector openness form a package. In a two-speed region where Riyadh and Abu Dhabi compete for gigawatt narratives, Manama can sell reliability of process: predictable hosting, clear transfer rules, and a role as a neutral interconnection point. That role is itself a sovereignty strategy—not sovereignty as self-sufficiency, but sovereignty as the capacity to set terms of access.

5.5 Implications for Security and Dual-Use Governance

AI compute is dual-use infrastructure. Training capacity relevant to civilian Arabic services is not neatly separable, at the hardware layer, from capacity relevant to more sensitive applications. Export-control regimes already encode that dual-use concern. Gulf governments that host large clusters therefore inherit obligations—political if not always legal—to prevent diversion, to manage insider threats, and to align cybersecurity baselines with the assurances they give partners. Data sovereignty rhetoric that ignores security governance will undercut the trust on which chip access depends.

At the same time, security governance can become a pretext for unnecessary centralisation that stifles university research and startup experimentation. A graded approach is preferable: high assurance for frontier-scale training clusters and government-sensitive workloads; lighter regimes for small-scale research and public open-source inference. Bahrain's government AI policy emphasis on legal compliance and awareness is compatible with such grading if followed by operational guidance that distinguishes risk tiers.

6. Policy Implications

6.1 Treat Compute Diplomacy as Core Foreign Policy

Compute diplomacy also has a South–South dimension. Microsoft and G42 have publicly described ambitions to extend AI and digital infrastructure to markets in the Middle East, Central Asia, and Africa. If Gulf hubs intermediate AI services into those markets, they inherit both influence and responsibility: for security standards, for data protection when services process foreign personal data, and for avoiding new dependencies that merely relocate chokepoints from California to the Gulf without improving end-user autonomy. A responsible hub strategy would include capacity-building and transparent documentation for partner governments.

Chip access and assurance agreements are now part of Gulf diplomacy with Washington and, indirectly, with other technology providers. Foreign ministries and economic ministries should institutionalise compute diplomacy: dedicated capacity to track export-control changes, negotiate assurance terms, and coordinate positions among GCC members where interests align. Publishing redacted model clauses for security assurances would help smaller agencies that lack G42- or HUMAIN-scale legal teams.

6.2 Build Layered Sovereignty Metrics

Governments should replace binary 'sovereign / not sovereign' scorecards with layered metrics along the four axes set out above—hosting, legal authority, organisational control, and model capability—plus an explicit fifth axis for upstream chip dependence. Honest dashboards reduce the risk that domestic audiences equate a ribbon-cutting at a data centre with strategic independence. They also clarify where cooperative GCC investment (for example, shared evaluation compute for Arabic models) would raise collective capability most efficiently.

6.3 Harmonise Transfer Rules without Erasing Experimentation

Full PDPL harmonisation across the GCC is unlikely in the short term and may be undesirable if it extinguishes useful experimentation such as Bahrain's data-embassy model or DIFC Regulation 10. A more realistic programme is mutual recognition for specified government and critical-infrastructure transfers, common documentation for high-risk automated systems, and shared incident-notification templates. Soft-law ethics manuals are a start; operational interoperability is the next step.

6.4 Keep Multi-Homing Options for Smaller States

Bahrain, Oman, Kuwait, and Qatar benefit from avoiding exclusive lock-in to a single hyperscaler or a single neighbour's AI champion. Procurement rules can require portability of logs, encryption-key escrow arrangements under domestic control, and tested exit plans. Multi-homing is not indecision; it is insurance in a choke-point economy.

6.5 Invest in Arabic Evaluation and Safety Public Goods

Arabic-language models are repeatedly cited as national differentiators. Their public value depends on shared evaluation datasets, safety benchmarks, and red-team protocols that no single firm will fully supply. GCC research institutions could jointly fund open evaluation suites for dialectal Arabic and for sectoral applications in health, education, and public services, reducing duplicated cost and raising bargaining power vis-à-vis global vendors.

6.6 Sequence Investments: Connectivity, Compliance, then Scale

For mid-sized and smaller GCC states, sequencing matters. Resilient connectivity and credible compliance systems should precede prestige-scale training builds. A well-audited mid-size region with clear transfer rules and tested exit options may deliver more sovereignty in practice than a larger cluster with weak identity management and unclear foreign-order handling. Scale amplifies both strength and mismanagement. Sequencing is therefore not conservatism; it is risk management under interdependence.

7. Conclusion

Future research should examine assurance agreements comparatively as instruments of economic statecraft, assess utilisation and evaluation quality of Arabic models under national champions, and trace how PDPL enforcement actions—still relatively young in several jurisdictions—shape AI procurement. Empirical work of that kind will refine, and may correct, the interpretive claims advanced here. What already seems clear is that the Gulf's AI future will be written not only in megawatts, but in licences, contracts, and the quiet legal engineering of where data is allowed to sit.

Gulf AI strategy is often narrated as a race to plant flags on compute campuses. The deeper contest is over the terms of interdependence. Local data centres, national champions, personal-data laws, and assurance agreements give Gulf states real instruments of control. US export controls, concentrated chip design, and hyperscale software ecosystems set hard limits on those instruments. Data sovereignty without borders names that condition without romanticising it.

For Bahrain, the lesson is to play to jurisdictional and trust advantages rather than to chase scale for its own sake. For the GCC, the lesson is that regional ethics manuals and bilateral mega-deals are not substitutes for interconnection standards and honest accounting of upstream dependence. Sovereignty in the age of AI compute is less about sealing borders than about knowing which borders still bite—and writing policy that bites back in the layers where Gulf states can actually win.

References

- Dubai International Financial Centre. (2023). Regulation 10 on personal data processed through autonomous and semi-autonomous systems. <https://www.difc.com/business/registrars-and-commissioners/commissioner-of-data-protection/regulation-10>
- Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, 44(1), 42–79. https://doi.org/10.1162/isec_a_00351
- Information & eGovernment Authority. (2025, July 27). Bahrain launches national AI policy and adopts GCC ethics manual. <https://www.iga.gov.bh/en/article/bahrain-launches-national-ai-policy-and-adopts-gcc-ethics-manual>
- Kingdom of Bahrain. (2018a). Law No. (30) of 2018 with respect to personal data protection law. <https://www.bahrain.bh/wps/wcm/connect/9956c467-1dd4-4bc6-a117-f88ca8f6f473/LAW+NO.+%2830%29+OF+2018+WITH+RESPECT+TO+PERSONAL+DATA+PROTECTION+LAW.pdf>

Kingdom of Bahrain. (2018b). Legislative Decree No. 56 of 2018 in respect of providing cloud computing services to foreign parties. <https://www.bahrainbusinesslaws.com/laws/Law-of-Providing-Cloud-Computing-Services-to-Foreign-Parties>

Microsoft. (2024, April 16). Microsoft invests \$1.5 billion in Abu Dhabi's G42 to accelerate AI development and global expansion. Microsoft Source. <https://news.microsoft.com/source/2024/04/16/microsoft-invests-1-5-billion-in-abu-dhabis-g42-to-accelerate-ai-development-and-global-expansion/>

Microsoft. (2025, November). Microsoft and G42 accelerate UAE's digital future with major data centre expansion. Microsoft Source EMEA. <https://news.microsoft.com/source/emea/2025/11/microsoft-and-g42-accelerate-uaes-digital-future-with-major-data-centre-expansion/>

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4). <https://doi.org/10.14763/2020.4.1532>

Public Investment Fund. (2025, May 12). HRH Crown Prince launches HUMAIN as global AI powerhouse. <https://www.pif.gov.sa/en/news-and-insights/press-releases/2025/hrh-crown-prince-launches-humain-as-global-ai-powerhouse/>

Saudi Data and AI Authority. (2023). Personal data protection law (English translation, reviewed version). <https://sdaia.gov.sa/en/SDAIA/about/Documents/PersonalDataProtectionLaw.pdf>

State of Qatar. (2016). Law No. 13 of 2016 on personal data privacy protection.

United Arab Emirates. (n.d.). UAE national strategy for artificial intelligence 2031. https://wp.oecd.ai/app/uploads/2021/12/United_Arab_Emirates_National_Strategy_for_Artificial_Intelligence_2017-2031.pdf

United Arab Emirates. (2021). Federal Decree-Law No. 45 of 2021 regarding the protection of personal data.

U.S. Bureau of Industry and Security. (2023, October 25). Implementation of additional export controls: Certain advanced computing items; supercomputer and semiconductor end use; updates and corrections. *Federal Register*, 88. <https://www.federalregister.gov/documents/2023/10/25/2023-23055/implementation-of-additional-export-controls-certain-advanced-computing-items-supercomputer-and>