

FROM OIL RENT TO COMPUTE POWER: ARTIFICIAL INTELLIGENCE, ISLAMIC GOVERNANCE AND STRATEGIC SECURITY IN THE GULF

Dr. ASIF MOHIUDDIN

Senior Lecturer, Department of Moral Studies, Civics and Character Building, Faculty of Human Sciences, Sultan Idris Education University, Malaysia.

Abstract

The Gulf's artificial intelligence (AI) boom is commonly framed as a project of economic diversification, yet it also raises questions of governance, security and technological dependence in states whose constitutional orders explicitly incorporate Islamic identity or principles. This article comparatively examines the development and governance of AI in Saudi Arabia, the United Arab Emirates (UAE) and Qatar, focusing on the relationship between hydrocarbon-derived state capacity, technological localisation and external dependence. Drawing on a structured analysis of public documents issued between 2017 and August 2026, including national AI strategies, ethics and cybersecurity frameworks, sovereign investment initiatives, corporate partnerships and export-control decisions, the study traces how financial and energy resources are being translated into computational infrastructure and domestic AI capability. It also examines how Islamic constitutional and normative commitments interact with the increasingly transnational language of AI governance. The analysis identifies distinct national trajectories within a common structural pattern. All three states have expanded domestic infrastructure, institutional capacity and bargaining leverage, yet continue to depend substantially on foreign semiconductors, cloud services, frontier AI models and externally governed technology supply chains. Islamic principles provide an important constitutional and normative foundation for ideas of public interest, responsibility, dignity and social order, but operational AI governance increasingly combines these commitments with internationally circulating ethical and regulatory frameworks. The article argues that Gulf AI development is producing neither straightforward technological sovereignty nor simple technological dependence. Instead, it reflects a form of negotiated technological autonomy in which localisation increases strategic capacity while simultaneously reorganising, rather than eliminating, dependence on external technology networks.

Keywords: Artificial Intelligence; Gulf Cooperation Council; Islam; Islamic Governance; Strategic Security; Technological Autonomy; Sovereign AI; Sovereign Wealth Funds.

1. INTRODUCTION

For much of the modern political economy of the Gulf, international leverage was associated with hydrocarbons: oil and gas generated fiscal rents, financed distributive states, enabled large infrastructure programmes and gave ruling institutions unusual capacity to act rapidly. The current AI boom does not displace that history. It redirects it. Saudi Arabia, the UAE and Qatar are using state capital, sovereign wealth, energy advantages and centralised institutions to acquire data centres, advanced accelerators, cloud capacity, models and technical partnerships. What is changing is therefore not the existence of rent-derived state power but the strategic asset into which it is being converted.

This transition also has a normative and institutional context that conventional diversification accounts often overlook. Saudi Arabia, the UAE and Qatar are not only resource-rich states and major investment powers; they are also political systems in

which Islam remains formally embedded in public authority, constitutional identity and wider understandings of social order. AI development in these states therefore takes place within environments where technological modernisation must coexist with established religious, ethical and institutional commitments. This does not mean that AI policy is simply an application of Islamic law, or that the three states approach religion and technology in the same way. Rather, it means that questions of innovation, legitimacy, responsibility and governance are negotiated within political cultures in which Islamic norms continue to shape the broader framework of public authority.

A third dimension is security. Advanced AI is inseparable from critical infrastructure, cyber resilience, data governance, semiconductor supply, cloud dependence and access to frontier models. The most advanced chips remain concentrated in global supply chains and can be subject to foreign export controls, licensing conditions, and security assurances. The strategic problem is therefore not simply whether Gulf states can finance compute, but whether physical localisation produces meaningful control when crucial hardware, software, platforms, and regulatory permissions remain external.

These three dynamics—resource conversion, Islamic governance and strategic security—are usually studied separately. Rentier-state and sovereign-wealth research explains the mobilisation of capital; digital-sovereignty research explains technological dependence; AI-governance scholarship addresses ethics and regulation; and emerging work on Islamic AI ethics considers how concepts such as *maṣlaḥa*, justice, dignity, responsibility and trusteeship can inform technological governance (Elmahjub, 2023). The analytical opportunity is to connect them without collapsing one into another. The central claim of this article is that Gulf AI strategy is a security project embedded in an Islamic governance environment, but its operational ethics are hybrid rather than exclusively religious. States draw legitimacy from national visions, constitutional identity, development promises and public-interest claims while governing AI through frameworks that also resemble global principles of fairness, transparency, privacy, accountability, safety, and human oversight.

The article asks three questions. First, how are Saudi Arabia, the UAE and Qatar converting hydrocarbon-derived financial power into domestic AI infrastructure and capability? Second, how is that transition governed in political orders with explicit Islamic constitutional identities? Third, does localisation generate strategic autonomy, or does it reorganise dependence on foreign technology networks? To answer these questions, the article develops two core concepts. Resource-to-compute conversion describes the transformation of state capital, sovereign assets, and energy advantages into AI infrastructure and institutional capability. Negotiated technological autonomy describes a condition in which a state gains domestic capacity and bargaining leverage while remaining embedded in external technological chokepoints.

The comparison identifies three pathways. Saudi Arabia follows a scale-and-localisation model built around SDAIA, PIF and HUMAIN. The UAE follows an integration-and-security model in which G42 and domestic institutions gain access to frontier capability through deep partnerships with US firms and government-to-government safeguards.

Qatar follows a niche-and-partnership model built around Arabic-language AI, ethical governance, local cloud capacity, and outward sovereign investment. None of these pathways produces technological autarky. Their significance lies instead in the ability to convert capital and political relationships into bargaining power, resilience, and selective control within an asymmetric AI stack.

2. ISLAM, GOVERNANCE AND THE SECURITY POLITICS OF AI

The Islamic dimension of Gulf AI policy should be treated carefully. It would be analytically weak to infer a direct religious origin for a technology policy simply because the state is constitutionally Islamic. Scholarship on Arab constitutionalism cautions against treating constitutional language as a self-executing policy code. Brown (2002) shows that Arab constitutions acquire political meaning through the institutions and practices that interpret them, while Lombardi (2013) demonstrates that constitutional clauses making *sharī'ah* “a” or “the” source of legislation vary substantially in legal history, interpretation, and practical effect. This article therefore treats Islamic constitutional identity as a governance and legitimacy context rather than as proof that individual AI rules are directly derived from fiqh.

Saudi Arabia provides the strongest constitutional formulation. Articles 1 and 8 of the Basic Law describe the Kingdom as a sovereign Arab Islamic state, identify the Qur'an and Sunnah as its constitution and state that governance is based on justice, consultation and equality in accordance with *sharī'ah* (Basic Law of Governance, 1992, arts. 1, 8). This does not convert the National Strategy for Data and AI into a fiqh document. It does, however, mean that the state's claims about responsible, beneficial and ethical AI sit within an order whose formal legal legitimacy is explicitly Islamic.

Qatar's constitutional arrangement is less encompassing but similarly explicit. Article 1 of the Permanent Constitution, as amended in 2024, identifies Islam as the state religion and *sharī'ah* as a principal source of legislation, while the amended text also adds consultation (*shūrā*), justice, and the rule of law to the description of the political system (Ministry of Justice, State of Qatar, 2024); Amiri Diwan, 2024). Article 5 links the state to the preservation of sovereignty, security, stability and territorial integrity (Permanent Constitution of the State of Qatar, 2004, as amended 2024, art. 5). Qatar's National AI Strategy is especially relevant because ethics is one of its six pillars, alongside education, data access, employment, business, and research (Ministry of Transport and Communications, State of Qatar, 2019). The result is not an explicitly *sharī'ah*-coded technical standard, but an institutional setting in which ethical AI is part of a national project whose constitutional identity is Islamic.

The UAE similarly combines an explicit Islamic constitutional foundation with internationally legible technology governance. Article 7 of the Constitution identifies Islam as the official religion of the federation and Islamic *sharī'ah* as a main source of legislation (Constitution of the United Arab Emirates, 1971, art. 7). Its AI ethics and security instruments, however, are framed largely in the language of fairness, accountability, transparency, explainability, robustness, safety, human-centred values, sustainability,

privacy and cybersecurity (Minister of State for Artificial Intelligence, Digital Economy and Remote Work Applications Office, 2022, 2024; United Arab Emirates Government, 2026). This is analytically important: Islamic constitutional identity and global AI-governance vocabularies coexist through institutional layering rather than through a single doctrinal source.

Beyond the constitutional setting, Islamic ethical thought offers several traditions that can illuminate AI governance without being treated as automatic policy sources. Opwis (2005) shows that *maṣlaḥa* has been interpreted differently across modern Islamic legal theory rather than functioning as a single, uncontested rule. Auda (2008) develops *maqāṣid al-sharīʿah* as a purposive and systems-oriented approach that foregrounds justice, dignity, common good and the consequences of legal and institutional arrangements. Elmahjub (2023) brings these traditions directly into AI ethics, arguing that *maṣlaḥa* and *maqāṣid* can support plural ethical benchmarking for questions such as privacy, fairness, transparency, autonomy and human welfare. This literature provides a richer basis for discussing Islamic governance than a one-to-one mapping between religious concepts and state policy.

For this article, these concepts are used interpretively and cautiously. The claim is not that SDAIA, G42, MCIT, or other Gulf institutions are implementing a single Islamic AI doctrine. Instead, Islamic ethical theory provides a vocabulary for evaluating the compatibility of technological modernisation with obligations concerning public benefit, justice, dignity, responsibility and the prevention of harm. Where official documents use similar language, the article treats this as normative compatibility unless the source itself establishes direct doctrinal borrowing.

This distinction matters for comparative research. If Islamic identity is treated only as symbolism, analysis misses the constitutional and legitimacy context of Gulf governance. If it is treated as the direct causal source of every AI rule, analysis overstates the evidence. The more defensible question is how Islamic constitutional identity, national-development ideology, international technical standards and security regulation coexist, reinforce one another, or create tensions in the governance of AI.

Alongside these constitutional and ethical dimensions, AI governance has moved beyond questions of innovation because compute infrastructure is becoming part of national security. Advanced models depend on high-performance chips, power, networks, cloud orchestration, training data, and cybersecurity. The UAE's National Cyber Security Policy for Artificial Intelligence explicitly treats AI systems as security-sensitive assets requiring governance, supply-chain risk management, model protection, operational resilience, adversarial-AI defence, monitoring, and incident response (United Arab Emirates Government, 2026). Saudi AI ethics guidance similarly links responsible AI to privacy, security, reliability, safety, transparency, and accountability (Saudi Data & AI Authority [SDAIA], 2023). Qatar's local deployment of Azure OpenAI is presented not simply as cloud adoption but as national-capability building with local data processing and enterprise-grade security (MCIT, 2025b).

The security politics of AI also arise from external control. Access to frontier semiconductors can be conditioned by export licences and security assurances. Cloud providers retain technical and contractual power over platforms even when data centres sit inside national territory. Model providers control updates, access conditions, and safety layers. Strategic autonomy therefore cannot be measured by the number of data centres alone. It requires attention to who controls the layers that make those facilities useful.

3. LITERATURE REVIEW AND RESEARCH GAP

The political-economy starting point remains the rentier state, but contemporary Gulf development increasingly relies on institutions that transform resource income into diversified assets. Sovereign wealth funds (SWFs) have evolved from passive reserve managers into active instruments of industrial policy, state capitalism, and international network building. Montambault Trudelle (2024) shows how Gulf SWFs can support regime adaptation and domestic development, while Korniyenko and Xin (2025) find that domestic and cross-border investment contributes to non-hydrocarbon growth across GCC economies. AI intensifies this developmental role because frontier computing requires high upfront capital, reliable energy, large-scale infrastructure, and patient financing.

The limitation of a purely diversification-centred lens is that investment volume does not reveal the location of control. A billion dollars spent on imported accelerators may increase domestic compute while also deepening dependence on a foreign architecture. A sovereign fund can own equity in a frontier AI company without acquiring control over its intellectual property or guaranteed access to its systems. Resource wealth is therefore an enabling condition, not an automatic measure of sovereignty.

A second strand of literature, on digital sovereignty, provides tools for disaggregating control. Roberts (2024) argues that AI sovereignty is relational and normative rather than reducible to physical ownership. Blancato (2024) similarly demonstrates how cloud localisation can coexist with strategic dependence on foreign providers. For the Gulf, this distinction is central: a data centre may be physically local, but its chips, cloud management layer, software dependencies, and frontier models can remain externally controlled.

Farrell and Newman's (2019) concept of weaponised interdependence adds a security dimension. Actors that control central network nodes can potentially use that position for surveillance, denial, or coercion. The Gulf cases do not show that dependence will necessarily be weaponised, but they do show that access is legally and politically conditioned. Export approvals for advanced chips, intergovernmental security assurances, and trusted-provider arrangements demonstrate that technological access is embedded in strategic relationships.

A third strand of scholarship has moved from broad digital-transformation narratives towards comparative AI governance. Albous, Al-Jayyousi and Stephens (2025) identify ambitious state-led AI strategies across the GCC, while Albous, Stephens and Al-

Jayyousi (2025) emphasise the importance of workforce readiness and institutional capability. Seloom (2026) brings securitisation directly into the analysis of Gulf AI governance, showing how exceptional and routine security practices can become intertwined in digital policy. These studies establish that infrastructure, regulation, and state power must be analysed together.

A parallel literature examines technological statecraft and Gulf agency. Miller and Wright (2025) show how the region navigates US-China AI competition, while Tran and Gulrez (2026) emphasise local agency and selective alignment rather than passive dependence. This scholarship is especially useful for explaining why close integration with US firms need not imply the absence of autonomy. States can gain leverage by becoming strategically valuable nodes in global networks.

The gap lies at the intersection of these literatures. Scholarship on Arab constitutionalism and Islamic legal theory explains why *sharī'ah*-source clauses cannot be read mechanically and why *maṣlaḥa* and *maqāṣid* are internally plural traditions (Brown, 2002; Lombardi, 2013; Opwis, 2005; Auda, 2008). AI-ethics scholarship has begun to translate those traditions into contemporary normative questions (Elmahjub, 2023), while Gulf AI studies focus more heavily on infrastructure, governance, labour and geopolitical alignment. Existing work rarely places Islamic constitutional identity, responsible-AI governance, resource-to-compute conversion and external security dependence in the same comparative framework. This article addresses that gap by treating Gulf AI as simultaneously a development strategy, a legitimacy project and a security architecture.

4. ANALYTICAL FRAMEWORK

Resource-to-compute conversion captures the transformation of hydrocarbon-derived fiscal resources, sovereign capital, energy advantages and state coordination into AI-related infrastructure and capability. The emphasis is on conversion rather than expenditure because comparable levels of investment may generate very different degrees of domestic technological capacity and external dependence. Relevant indicators include data-centre infrastructure, access to advanced processors and networking, cloud platforms and software, data and model capabilities, technical labour, research institutions and firms capable of deploying AI across government and the wider economy. The depth of this conversion depends on the coordination of investment, procurement, research, regulation and deployment, as well as on the structure of relationships with foreign technology firms and supplier states. Localisation may remain relatively shallow where domestic activity is confined to hosting imported infrastructure, or extend more deeply into operational control, specialised expertise, model development, intellectual property and the capacity to substitute external suppliers. These distinctions provide a basis for assessing whether large-scale AI investment is generating domestic capability or primarily reinforcing reliance on externally controlled technological systems.

Negotiated technological autonomy describes the strategic position that emerges from this process. It refers to the capacity to pursue national technological objectives and

reduce vulnerability to external denial while remaining embedded in international technology networks. Autonomy is therefore neither equivalent to technological self-sufficiency nor incompatible with dependence. It may increase where domestic expertise expands, suppliers become more diversified, alternative technological pathways become credible and the state acquires sufficient strategic value to influence the terms on which technology is accessed.

Comparison across Saudi Arabia, the UAE and Qatar consequently centres on infrastructure localisation, supplier diversification, domestic technical capability, exposure to foreign regulatory and export-control regimes and bargaining capacity in relations with technology providers and governments. These dimensions make it possible to distinguish between dependence that is concentrated and difficult to replace and dependence that is diversified, negotiable or partially offset by domestic capability. Material and strategic autonomy alone, however, do not capture how AI is governed within Gulf political orders. Normative-governance fit addresses the relationship between technological development and the ethical, legal and public-interest principles through which state authority is justified. In Saudi Arabia, the UAE and Qatar, this relationship is especially significant because Islamic identity and principles remain constitutionally embedded while contemporary AI governance also draws on internationally circulating concepts such as responsibility, transparency, dignity, harm prevention and public welfare.

Islamic security governance provides a narrower interpretive lens within this dimension. It does not imply the existence of a unified Islamic model of AI or cybersecurity governance. Rather, it captures the interaction between Islamic constitutional ordering, state responsibility for security and public welfare, and contemporary systems of technological regulation. The relevant concern is not simply whether religious language appears in AI policy documents, but whether ethical, legal and security mechanisms are situated within a broader constitutional order in which Islamic principles continue to shape state legitimacy and normative authority.

These concepts connect three aspects of Gulf AI development that are often examined separately: the conversion of financial and energy resources into computational capability, the extent to which that capability alters relations of technological dependence, and the governance structures through which AI is made compatible with domestic political and normative orders. The framework therefore enables comparison not only of how much AI capacity each state is building, but also of the depth of localisation, the strategic consequences of continued external dependence, and the institutional and normative conditions under which that technological expansion is governed.

5. RESEARCH DESIGN AND METHODOLOGY

This study employs a structured, focused comparison of Saudi Arabia, the United Arab Emirates (UAE), and Qatar between 2017 and August 2026. The period captures the emergence and consolidation of national AI strategies across the three states, beginning with the UAE's 2017 strategy and followed by Qatar's 2019 strategy. The cases share several structural characteristics, including hydrocarbon wealth, substantial sovereign

financial capacity, state-led development, and close engagement with global technology firms. At the same time, they differ in population size, institutional arrangements, AI-ecosystem maturity, and external partnership structures. These similarities and differences make them suitable for examining how comparable resource advantages generate distinct pathways towards technological autonomy.

The analysis draws on a corpus of primary public documents and relevant scholarly literature. The primary corpus comprises constitutional and constitutional-amendment texts; national AI strategies and ethics frameworks; cybersecurity and data-governance instruments; official announcements concerning sovereign investment and AI infrastructure; and government and corporate documents relating to cloud services, advanced semiconductors, frontier models, and international technology partnerships. These include materials issued by Saudi Arabia's SDAIA and PIF; the UAE Government and the Minister of State for Artificial Intelligence, Digital Economy and Remote Work Applications Office; Qatar's Ministry of Communications and Information Technology and Qatar Investment Authority; and technology partners including Microsoft, NVIDIA, AMD, and OpenAI. U.S. Department of Commerce documents are also included where access to advanced computing infrastructure is conditioned by export-control or security arrangements. Constitutional sources comprise Saudi Arabia's Basic Law, the UAE Constitution, and Qatar's Permanent Constitution and related 2024 amendment materials.

The scholarly literature provides the conceptual and interpretive basis for the comparison. It covers rentier political economy and sovereign wealth, digital and technological sovereignty, strategic interdependence, Gulf AI governance, Arab constitutionalism, Islamic legal and ethical thought, and contemporary AI ethics. These sources are used to develop the concepts of resource-to-compute conversion and negotiated technological autonomy and to situate the empirical findings within wider debates on technological dependence, governance, and normative legitimacy.

Each primary source was analysed through a common coding framework. The principal dimensions included country and date, document type, project status, resource-to-compute layer, infrastructure localisation, supplier diversification, domestic capability, regulatory exposure, and bargaining capacity. The resource-to-compute dimension distinguishes among capital and energy inputs, data-centre infrastructure, semiconductors, cloud and software, models and data, and skills and research capacity. Additional interpretive dimensions capture the interaction between Islamic constitutional identity and contemporary governance principles, as well as the security significance of specific policies, infrastructure projects, and international partnerships.

External technological dependence is assessed through a qualitative comparative framework. Dependence is classified as high where at least two of three conditions are present: a critical frontier input is controlled or produced outside the state; access is materially affected by foreign export licensing, corporate platform jurisdiction, or external security conditions; and no publicly verified domestic or readily substitutable frontier-equivalent alternative is available. Moderate dependence indicates continuing external

control alongside a credible diversification or substitution pathway, while **low dependence** requires substantial domestic control together with viable alternatives for critical technological inputs. These categories are not intended to function as a numerical sovereignty index. They provide a consistent basis for comparing how localisation, investment, institutional capacity, and international partnerships alter exposure to external technological constraints while potentially increasing domestic bargaining power and operational room for manoeuvre.

The comparative framework is applied to the principal AI infrastructure, investment and capability-building initiatives identified across the three cases. Table 1 provides an empirical overview of these initiatives, distinguishing national strategy targets, announced infrastructure projects, corporate partnerships and authorised access to advanced computing resources. The table is not intended to rank the three states by investment scale. Rather, it illustrates the different ways in which financial resources, state coordination and external partnerships are being converted into domestic AI capacity, while also indicating where that capacity remains dependent on foreign technologies, suppliers or regulatory approval.

Table 1: AI Infrastructure and Investment Commitments

Country / initiative	Figure	Status in source	Strategic significance
Saudi Arabia – National Strategy for Data & AI	~SAR 75 billion targeted data/AI investment; 20,000+ specialists; 300+ startups by 2030	National strategy target	Links AI to long-term state capacity, skills, investment, and diversification.
Saudi Arabia – HUMAIN/NVIDIA	Up to 500 MW; first announced phase: an AI supercomputer incorporating 18,000 NVIDIA GB300 Grace Blackwell GPUs	Planned over five years	Very large localisation ambition, but dependent on NVIDIA hardware.
Saudi Arabia – HUMAIN/AMD	Up to US\$10 billion; up to 500 MW over five years	Planned multiyear collaboration	Potential vendor diversification; figures should not be assumed additive with NVIDIA plan.
Saudi Arabia & UAE – US chip approvals	Each company authorised for equivalent of up to 35,000 NVIDIA GB300 chips	Authorised subject to security/reporting conditions	Shows that compute access remains dependent on US regulatory permission.
UAE – UAE-US AI campus	Planned 5 GW campus; Phase 1 begins with 1 GW	Planned / Phase 1 announced	Positions UAE as regional compute hub under government-to-government security framework.
UAE – Stargate UAE	1 GW cluster; 200 MW expected to go live in 2026	Planned within broader campus	Deep integration with OpenAI, G42, Oracle, NVIDIA, Cisco, and SoftBank.

Country / initiative	Figure	Status in source	Strategic significance
UAE – Microsoft/G42	US\$1.5 billion Microsoft investment in G42	Announced investment (2024)	Combines capital and cloud access with formal intergovernmental assurance requirements.
Qatar – Qai/Brookfield	US\$20 billion strategic AI-infrastructure joint venture	Announced (2025)	Moves Qatar toward co-owned infrastructure and integrated compute facilities.
Qatar – Fanar	At least 300 billion Arabic words planned for model data corpus	Official project specification	Targets Arabic-language and cultural capability rather than only raw compute scale.
Qatar – Azure expansion	Additional 4 MW and 6 MW capacities for Azure Qatar data centre	Agreement announced (2025)	Concrete local cloud expansion; still embedded in Microsoft platform.

Note. Figures are reported as described by the issuing organisation and are not summed where projects may overlap. Sources: SDAIA (2020); NVIDIA (2025); Advanced Micro Devices (2025); U.S. Department of Commerce (2025a–c); Microsoft (2024); OpenAI (2025); QIA (2025); MCIT (2024, 2025a, 2025b).

The initiatives in Table 1 show that resource-to-compute conversion is occurring through different combinations of infrastructure scale, institutional coordination, specialised capability and international partnership. They also reveal an important tension that recurs across the cases: localisation can increase domestic capacity without necessarily transferring control over the technological layers on which that capacity depends. The following country analyses examine how this relationship develops in Saudi Arabia, the UAE and Qatar, with particular attention to the interaction between resource mobilisation, governance arrangements and continuing external dependence.

6. SAUDI ARABIA: ISLAMIC STATE CAPACITY, SCALE AND FULL-STACK AMBITION

Saudi Arabia represents the most concentrated attempt to transform state resources into a vertically integrated AI platform. SDAIA’s National Strategy for Data and AI sets a 2030 ambition to place the Kingdom among leading AI economies, attract approximately SAR 75 billion in investment, develop more than 20,000 specialists and experts, and create more than 300 startups (SDAIA, 2020). The strategy explicitly connects data and AI to Vision 2030, infrastructure, research, skills, public services, energy, healthcare, and economic diversification.

The ethical dimension has become more institutionalised over time. SDAIA’s AI Ethics Principles emphasise integrity and fairness, privacy and security, reliability and safety, transparency and interpretability, and accountability and responsibility (SDAIA, 2023). In the Islamic constitutional setting established in Section 2, these principles connect responsible AI to a broader state commitment to public benefit, accountability, and protection from harm without constituting a separate fiqh-based AI code.

The launch of HUMAIN in May 2025 concentrated the infrastructure side of this strategy. PIF created HUMAIN as a full-stack AI company spanning data centres, infrastructure, cloud, advanced models, and applications (Public Investment Fund [PIF], 2025). The model is significant because it combines sovereign capital with central coordination. It also links AI development to the Saudi state's ability to mobilise land, energy, finance, industrial policy, and diplomatic relationships at scale.

The NVIDIA and AMD announcements illustrate this resource-to-compute logic. HUMAIN and NVIDIA announced a projected build-out of up to 500 MW over five years using several hundred thousand advanced GPUs, with the first announced phase centred on an AI supercomputer incorporating 18,000 NVIDIA GB300 Grace Blackwell GPUs (NVIDIA, 2025). AMD and HUMAIN separately announced a collaboration of up to US\$10 billion and up to 500 MW over five years using AMD compute and the ROCm software ecosystem (Advanced Micro Devices, 2025). These are extraordinary figures, but they remain commitments rather than proof of completed capacity.

Saudi strategy also exposes the autonomy problem most clearly. The United States' November 2025 authorisation for HUMAIN to acquire the equivalent of up to 35,000 GB300 chips expanded access while making that access conditional on rigorous security and reporting requirements (U.S. Department of Commerce, 2025a). Physical localisation therefore coexists with regulatory dependence. The data centre may be in the Kingdom, but the highest-end chips are imported and subject to foreign controls. This arrangement nevertheless gives Saudi Arabia bargaining power. Capital, energy, market size and state-backed procurement make the Kingdom commercially important to multiple vendors. The presence of NVIDIA and AMD relationships also creates some ecosystem plurality, even if both remain US-origin suppliers. Saudi autonomy should therefore be understood as leverage within interdependence rather than independence from it.

The security dimension extends beyond hardware. As AI becomes integrated into government, energy, healthcare, mobility and public administration, failure, misuse, or compromise can affect national resilience. SDAIA's ethics framework and national data-governance infrastructure indicate that the state is building normative and technical controls alongside compute capacity. The Saudi pathway is therefore best described as state-concentrated Islamic developmentalism applied to AI: centralised resource mobilisation, ethical-administrative governance, and a strategic attempt to localise compute without abandoning foreign partnerships.

7. UNITED ARAB EMIRATES: STRATEGIC INTERDEPENDENCE, AI SECURITY, AND GLOBAL HUB GOVERNANCE

The UAE entered the current AI cycle with a more mature institutional ecosystem and an earlier national strategy. Its 2017 AI strategy framed AI as a tool for government performance, sectoral transformation, and long-term competitiveness (United Arab Emirates Government, 2017). Abu Dhabi subsequently developed a dense institutional network including G42, the Mohamed bin Zayed University of Artificial Intelligence, sovereign investment vehicles, and partnerships with leading international firms.

The UAE's Islamic constitutional setting, outlined in Section 2, operates alongside an internationally legible technology-governance framework. Its AI Ethics Principles and Guidelines emphasise fairness, accountability, transparency, explainability, robustness, safety, human-centred values, and sustainability, while the 2024 AI Charter adds responsible use, privacy, data security, inclusion, and legal compliance (Minister of State for Artificial Intelligence, Digital Economy and Remote Work Applications Office, 2022, 2024). The result is a hybrid governance vocabulary rather than a distinct religious technical code.

Security is especially explicit in the UAE case. The National Cyber Security Policy for Artificial Intelligence requires governance for AI/ML systems, supply-chain risk management, infrastructure and application security, model and algorithm protection, operational safety, adversarial-AI defence, monitoring, response, and digital forensics (United Arab Emirates Government, 2026). This policy moves the UAE beyond general responsible-AI principles toward a national-security treatment of AI systems as critical assets.

The Microsoft-G42 partnership demonstrates how this security logic shapes external integration. Microsoft's US\$1.5 billion investment in G42 gives the UAE access to Azure-based infrastructure and global distribution, but the partnership is governed by an Intergovernmental Assurance Agreement and commitments to US and international trade, security, and responsible-AI standards (Microsoft, 2024). The arrangement therefore converts geopolitical trust into technological access.

The same logic appears in the UAE-US AI Acceleration Partnership and the planned 5-GW campus in Abu Dhabi. The US Department of Commerce announced that Phase 1 would begin with a 1-GW data centre within a planned 5-GW cluster, with G42 leading a consortium and US partners providing major components of the technology stack (U.S. Department of Commerce, 2025b, 2025c). OpenAI's Stargate UAE adds a 1-GW cluster, with 200 MW expected to go live in 2026, and explicitly situates the project within coordination with the US government (OpenAI, 2025). These figures should not be double-counted because Stargate is part of the broader campus architecture.

The UAE's model might appear less autonomous because its security conditions are formalised. Yet that interpretation is incomplete. Formalisation can also stabilise access. By accepting technology-protection commitments, the UAE becomes a trusted hub for infrastructure that might otherwise remain concentrated in the United States. Strategic interdependence can therefore increase effective autonomy if it provides predictable access, domestic operating capacity, and a role in regional deployment.

The UAE pathway is thus based on regulated integration. It uses local institutions and capital to become indispensable enough that leading firms and governments are willing to share high-end capability under negotiated safeguards. Islamic constitutional identity supplies the national normative background; global AI ethics supplies the operational language; cybersecurity policy translates AI into national-security governance; and strategic partnership delivers the compute.

8. QATAR: ETHICAL GOVERNANCE, ARABIC CAPABILITY AND PORTFOLIO AUTONOMY

Qatar's pathway is shaped by smaller demographic and market scale but exceptionally strong financial capacity. Within the Islamic constitutional setting described in Section 2, its 2019 National AI Strategy is distinctive because ethics is one of six formal pillars alongside education, data access, employment, business, and research. The strategy seeks both the capacity to produce AI applications in areas of national interest and the institutional ability to adopt AI through education, law, and ethical guidance (MCIT, 2019).

This gives Qatar a distinctive normative profile: ethics is embedded in the original strategy architecture rather than added after infrastructure development. Subsequent MCIT initiatives have extended this responsible-AI orientation, linking technological development to national development and social welfare without presenting it as a state-declared Islamic AI jurisprudence.

Fanar illustrates Qatar's preference for niche capability. MCIT describes the project as an Arabic generative AI initiative intended to address the gap between Arabic and English AI performance and to provide culturally resonant content.

The project was designed around a high-accuracy Arabic corpus of at least 300 billion words (MCIT, 2024). The strategic importance of Fanar lies less in competing with the largest frontier models by parameter count than in building national and regional capability in language, culture, data curation, and public-sector use.

Qatar's infrastructure strategy relies more openly on partnership. In February 2025, MCIT announced that Azure OpenAI services would be available through Microsoft's Qatar data-centre region, with advanced OpenAI models running on Azure and data processing occurring locally in the Microsoft cloud region (MCIT, 2025b).

The arrangement increases data residency and local access but does not transfer ownership of the cloud or model stack. This is a clear example of negotiated technological autonomy: control increases at some layers while dependence persists at others.

The creation of Qai and its US\$20 billion joint venture with Brookfield moved the strategy toward more direct infrastructure ownership. The venture is intended to develop integrated AI facilities in Qatar and selected international markets while supporting domestic skills and supply chains (Qatar Investment Authority [QIA], 2025).

In December 2025, MCIT also announced an expansion of the Azure Qatar data centre through additional capacities of 4 MW and 6 MW with MEEZA, providing a rare concrete measure of incremental cloud capacity (MCIT, 2025a).

Qatar's sovereign investment strategy adds another layer of optionality. QIA's investments in frontier technology firms can build commercial relationships and exposure to innovation even when they do not create sovereign rights over intellectual property. The distinction is important: equity ownership is not technological control. Yet portfolio relationships can still improve access to information, partnerships, and future opportunities.

Qatar therefore represents a niche-and-portfolio pathway. Its Islamic constitutional identity and ethics-oriented national strategy provide a strong normative frame; Arabic AI creates differentiated capability; local cloud deployment improves data residency; and sovereign investment broadens external connections. The strategy is less focused on headline megawatt scale than Saudi Arabia or the UAE, but it may produce resilience through specialisation and diversified partnerships.

9. COMPARATIVE ANALYSIS

Table 2: Comparative Pathways from Resource Wealth to Strategic AI Capacity

Dimension	Saudi Arabia	United Arab Emirates	Qatar
Dominant pathway	Scale and localisation	Regulated strategic interdependence	Niche capability and portfolio partnership
Core state vehicles	SDAIA; PIF; HUMAIN	G42; federal/Abu Dhabi institutions; sovereign investors	MCIT; QIA; Qai; QCRI/HBKU
Islamic-governance relationship	Strong constitutional Islamic foundation; AI ethics operationalised through SDAIA principles	Islamic constitutional foundation combined with internationally framed AI ethics and mixed legal governance	Islamic constitutional foundation; ethics explicitly included in national AI strategy
Security architecture	Data governance, privacy/security principles, export-controlled chip access	Dedicated AI cybersecurity policy; intergovernmental assurance and technology-protection commitments	Ethics, local processing, trusted AI infrastructure, security/stability constitutional context
Primary autonomy asset	Scale, energy, capital, vendor attraction	Trusted-hub status, mature institutions, deep US integration	Arabic specialisation, local cloud, sovereign portfolio optionality
Main external vulnerability	Advanced chips, software ecosystems, export licensing	US chips/cloud/models and formal compliance conditions	Foreign cloud/models, advanced chips, operating expertise

Note. The comparison is interpretive and based on public evidence through August 2026. It distinguishes domestic assets from externally controlled layers.

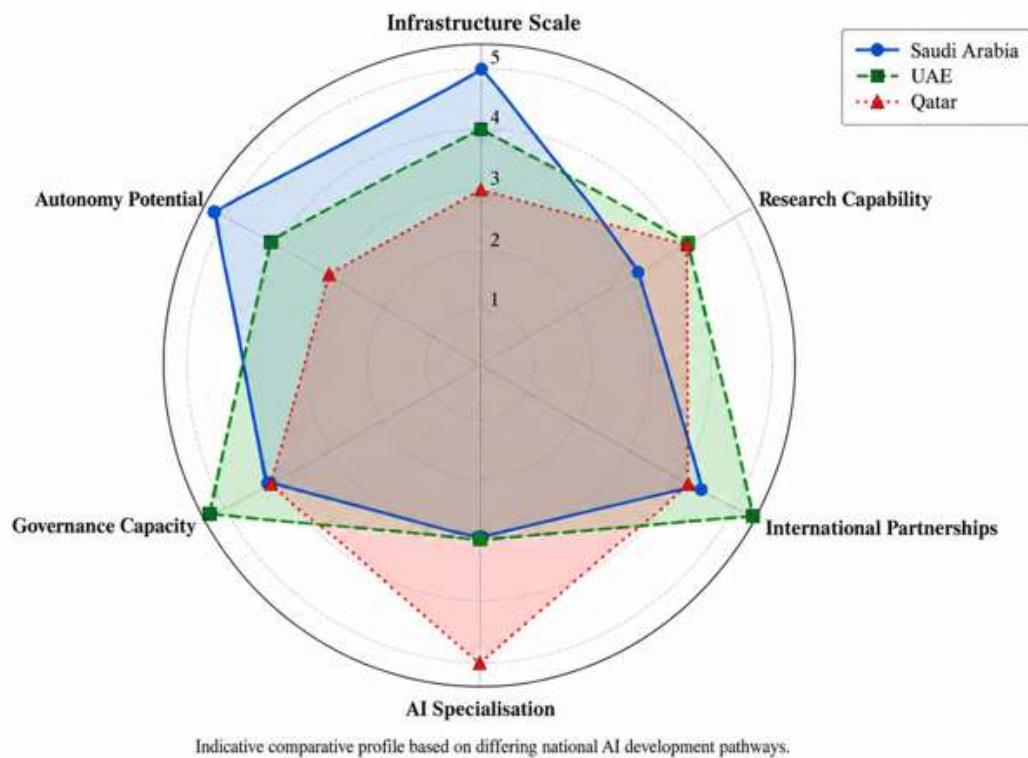


Figure 1: Comparative AI Development Profiles of Saudi Arabia, UAE and Qatar

Figure 1 provides a visual comparison of the different AI development pathways pursued by Saudi Arabia, the UAE and Qatar. The profile does not represent a ranking of overall AI performance; instead, it highlights the strategic emphasis of each national pathway. Saudi Arabia's stronger infrastructure scale and autonomy potential reflect its focus on large-scale localisation and state-backed compute development. The UAE profile illustrates the importance of international partnerships and governance capacity in building a globally connected AI ecosystem. Qatar's pattern reflects a specialised approach, with greater emphasis on AI specialisation and targeted capability development. The figure demonstrates that Gulf AI strategies differ in their sources of leverage, even though all three states continue to operate within internationally dependent technology networks.

Table 2 summarises the three national pathways and shows that resource wealth converts more readily into compute capacity than into full technological sovereignty. The cases differ in the sources of leverage they develop, but all remain exposed to critical upstream technologies and external conditions.

Figure 2 illustrates why physical localisation of AI infrastructure does not automatically translate into complete technological control. The layered structure shows that domestic influence is generally stronger in areas such as data governance and application deployment, while deeper technological layers, particularly advanced semiconductors and parts of the model ecosystem, remain more exposed to external suppliers. This

layered perspective complements the country comparison by showing that technological autonomy depends not only on the presence of infrastructure but also on control across the different components of the AI value chain.

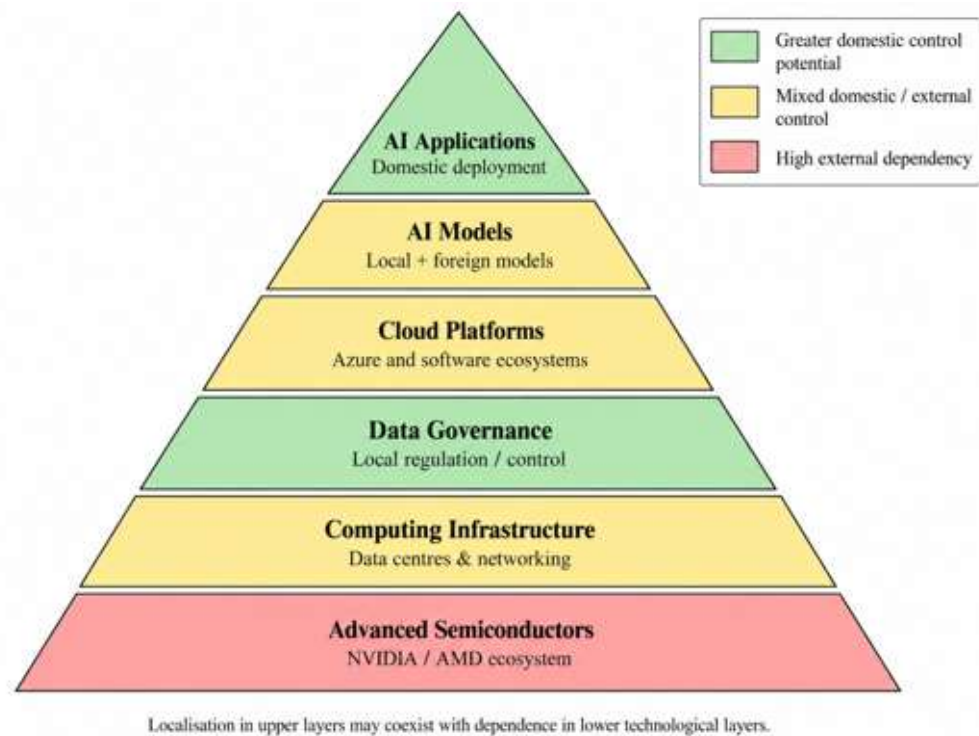


Figure 2: AI Technology Stack and External Dependency Layers

Security is the strongest point of convergence. Privacy, cyber resilience, supply-chain integrity, model security, export controls, and trusted-provider arrangements all function as mechanisms for keeping AI politically and operationally governable. Table 3 shifts the comparison from national pathways to the technological layers at which dependence and security exposure remain most significant.

Table 3: Layered Dependence and Security Exposure

Layer	Saudi Arabia	United Arab Emirates	Qatar	Security implication
Advanced semiconductors	High external dependence	High external dependence	High external dependence	Foreign licensing and supply-chain concentration can constrain scale and timing.
Cloud platforms	Multiple foreign partners; localisation growing	Deep Azure and US-provider integration	Azure local region central to advanced model access	Data residency does not equal platform sovereignty.

Layer	Saudi Arabia	United Arab Emirates	Qatar	Security implication
Frontier models	Domestic/Arabic ambitions plus foreign ecosystems	Strong foreign-model partnerships plus domestic research	Fanar for Arabic use; foreign frontier models via Azure	Model access, updates, and safety controls can remain externally governed.
Data and governance	Strong state data authority and ethics framework	Strong ethics + dedicated AI cybersecurity architecture	Ethics pillar, local processing, national strategy	Domestic governance can reduce some vulnerabilities even when hardware remains foreign.
Capital and infrastructure	Very high bargaining capacity	Very high bargaining capacity and hub value	Very high sovereign capital but smaller market	Capital creates leverage but not ownership of technological chokepoints.

Note. “High external dependence” is assigned when at least two of three conditions are documented: foreign control of a critical frontier input; material exposure to foreign licensing, platform jurisdiction, or security conditions; and absence of a publicly verified domestic or readily substitutable frontier-equivalent alternative by 31 August 2026. The rating indicates structural exposure, not an absence of domestic capability, and is a comparative documentary judgment rather than a numerical index.

10. DISCUSSION

The comparison shows that the Gulf AI boom is more than an extension of economic diversification. It is an attempt to convert resource-derived financial power into technological and institutional capacity. HUMAIN’s announced first-phase supercomputer incorporating 18,000 NVIDIA GB300 Grace Blackwell GPUs, the UAE’s planned 5-GW AI campus and Qatar’s Fanar initiative represent different routes through which capital, infrastructure, institutions, and specialised knowledge are being assembled into domestic AI capacity (MCIT, 2024; NVIDIA, 2025; U.S. Department of Commerce, 2025b, 2025c). These examples matter not simply because of their size, but because they reveal different mechanisms of resource-to-compute conversion: Saudi Arabia prioritises scale and vertically coordinated infrastructure, the UAE combines hub-building with deeply institutionalised external partnerships, and Qatar places greater emphasis on specialised Arabic capability and portfolio-based access.

Yet investment volume cannot be treated as a measure of technological sovereignty. Saudi Arabia’s compute plans remain dependent on foreign processors and software ecosystems; the UAE’s frontier capacity is deeply embedded in partnerships with US technology firms; and Qatar’s locally hosted Azure services improve data residency without transferring ownership of the cloud or frontier-model stack (Advanced Micro Devices, 2025; MCIT, 2025b; Microsoft, 2024; NVIDIA, 2025). The November 2025 US authorisations for HUMAIN and G42 further demonstrate that access to critical frontier

inputs can remain externally conditioned by security and reporting requirements (U.S. Department of Commerce, 2025a).

These cases reveal a localisation paradox. Domestic data centres can improve data residency, generate specialised employment, support technical learning, and give governments greater influence over national deployment. Domestic companies such as HUMAIN and G42 can accumulate expertise and bargaining capacity, while local models can address linguistic and cultural gaps. Qatar's Fanar project is significant in this respect because its planned Arabic corpus represents capability-building through linguistic and cultural specialisation rather than only scale (MCIT, 2024). Localisation also shortens some infrastructure chains, attracts technology firms, and can create institutional vehicles through which governments learn how to procure, operate, and regulate advanced systems. Its significance is therefore not exhausted by the geographic location of servers; it also lies in whether repeated deployment creates cumulative organisational and technical competence.

Localisation can nevertheless deepen dependence at other layers. Investment in NVIDIA or AMD hardware embeds infrastructure within particular processor and software ecosystems, while Azure-based expansion can increase local cloud capacity and reliance on Microsoft's platform. Proprietary architectures can also raise switching costs through software migration, workforce retraining, procurement changes, and new operating procedures. This reflects the wider digital-sovereignty problem identified by Blancato (2024) and Roberts (2024): physical localisation can reduce vulnerability in one part of the stack while increasing it elsewhere. Table 3 therefore supports assessing autonomy by the distribution of control across technological layers rather than by installed capacity alone. The point is not that dependence simply increases as localisation proceeds. Rather, the composition of dependence changes: governments may gain more control over siting, data handling, deployment, and procurement while becoming more exposed to specific chip architectures, cloud environments, or model providers. This layered redistribution of control is analytically more important than a binary classification of sovereign versus dependent.

This layered pattern explains why negotiated technological autonomy is more useful than a simple sovereignty/dependence distinction. Autonomy does not require domestic control of every component in a globally concentrated technology stack. More relevant is whether states can diversify suppliers, adapt systems to domestic needs, retain critical data, build expertise, negotiate favourable access conditions, and maintain essential services when external conditions change. This is consistent with relational approaches to AI and digital sovereignty that emphasise degrees of control, bargaining power, and interdependence rather than complete technological self-sufficiency (Roberts, 2024).

Technological autonomy is also distinct from governance autonomy. The former concerns the capacity to develop, access, maintain, substitute, and negotiate control over critical technological resources; the latter concerns the authority of public institutions to determine the legal, ethical, security, and social conditions under which those technologies are used. A state may rely heavily on foreign hardware and software while

retaining substantial authority over data protection, procurement, cybersecurity, public-sector deployment, and institutional oversight. Conversely, domestic ownership of infrastructure does not by itself guarantee effective accountability or protection from technological harm.

This distinction matters because Gulf AI strategies combine strong domestic state authority with extensive technological interdependence. Semiconductor security requirements, the assurance framework surrounding Microsoft's relationship with G42, and reliance on international platforms show that technological access can remain externally conditioned (Microsoft, 2024; U.S. Department of Commerce, 2025a). At the same time, Saudi Arabia, the UAE, and Qatar retain significant authority over deployment priorities, data regulation, cybersecurity practices, public-sector applications, and ethical frameworks. As AI becomes embedded in administration, healthcare, education, energy, mobility, and cybersecurity, governance autonomy therefore depends on institutions being able to determine permissible uses, accountability arrangements, incident response, and continuity of essential services even where the underlying technology is not fully domestically controlled. This distinction is especially consequential where governments must investigate model errors, assign responsibility across public and private actors, impose cybersecurity requirements, and preserve service continuity when suppliers or geopolitical conditions change. Governance capacity therefore remains a meaningful form of autonomy even where technological substitution remains limited.

Security further complicates the relationship between localisation and control. The UAE's National Cyber Security Policy for Artificial Intelligence treats AI systems as security-sensitive assets and addresses supply-chain risk management, model protection, infrastructure and application security, adversarial-AI defence, monitoring, incident response, and operational resilience (United Arab Emirates Government, 2026). This illustrates a broader shift in Gulf AI policy: computational infrastructure is increasingly treated not merely as an economic asset but as part of national-security architecture.

The security implications extend beyond cyber threats. Large AI facilities depend on continuous electricity, cooling, network connectivity, replacement hardware, software support, and reliable international supply chains. Concentrated computing capacity can therefore remain vulnerable even when facilities are domestically owned. A local data centre does not provide meaningful strategic autonomy if replacement chips cannot be obtained, essential software cannot be maintained, or failures elsewhere in the technological chain disrupt operations. In this sense, the Gulf cases reinforce the insight from weaponized-interdependence scholarship that control over critical network nodes can create political leverage even where economic relationships remain mutually beneficial (Farrell & Newman, 2019). Resilience should therefore form part of the assessment of technological autonomy alongside ownership and localisation.

The Gulf cases also complicate assumptions about the role of Islam in technological governance. The evidence does not show the emergence of a unified Islamic AI regulatory model, but neither does it support treating Islamic constitutional identity as merely symbolic. Instead, the three states display normative layering in which Islamic

constitutional foundations coexist with internationally recognisable AI-ethics principles, national-development strategies, cybersecurity rules, corporate governance arrangements, and technical standards. This layering is visible in the ethical vocabulary used by Gulf institutions. Saudi Arabia's AI Ethics Principles emphasise integrity and fairness, privacy and security, reliability and safety, transparency and interpretability, and accountability and responsibility (SDAIA, 2023). UAE frameworks similarly emphasise fairness, transparency, accountability, explainability, privacy, safety, sustainability, and human-centred governance (Minister of State for Artificial Intelligence, Digital Economy and Remote Work Applications Office, 2022, 2024), while Qatar incorporated ethics as one of six pillars of its National AI Strategy (MCIT, 2019). These frameworks are not presented as direct applications of classical fiqh; their operational language is closely aligned with international AI-governance discourse.

Islamic ethical concepts nevertheless remain analytically relevant as normative resources rather than mechanically applicable policy rules. *Maṣlaḥa*, justice, dignity, responsibility and prevention of harm can inform questions of discrimination, privacy, surveillance, human oversight, accountability and the distribution of technological benefits. Islamic legal and ethical scholarship itself cautions against treating *maṣlaḥa* or *maqāṣid* as singular doctrines, while contemporary work demonstrates how these traditions can inform plural ethical benchmarking for AI (Auda, 2008; Elmahjub, 2023; Opwis, 2005). The resulting pattern is best understood as selective synthesis: Islamic constitutional identity provides one normative layer, internationally circulating responsible-AI standards another, while cybersecurity, data regulation, development policy, and corporate governance add further layers. This approach also avoids two opposite interpretive errors already identified in Section 2: treating every AI policy as a direct expression of Islamic law, or treating Islam as irrelevant because operational standards employ internationally familiar language. The analytical question is how these normative and institutional layers interact in practice, and whether broad principles of justice, dignity, accountability, privacy, and harm prevention are translated into enforceable governance mechanisms.

The comparison further suggests that resource-to-compute conversion is cumulative rather than instantaneous. Hydrocarbon wealth provides initial financial capacity, but capital alone does not produce durable technological power. Financial resources fund energy systems, data centres, processors, cloud services, research institutions, and AI companies; these assets can then attract firms and specialised labour, develop technical and organisational knowledge, and gradually strengthen bargaining power.

Saudi Arabia illustrates this process at very large scale. Sovereign capital and state coordination have enabled HUMAN and major infrastructure partnerships, but their long-term strategic value will depend on whether they generate domestic technical expertise, research capability, software competence, and firms able to maintain and adapt systems rather than merely operate imported technologies. NVIDIA's announcement links infrastructure expansion to training and skills development (NVIDIA, 2025). The UAE's earlier institutional development around G42 and the Mohamed bin Zayed University of Artificial Intelligence provides a broader organisational base for linking infrastructure,

research, and skills, while Qatar's Fanar initiative demonstrates that capability-building can also occur through specialised data, linguistic expertise, and model development rather than scale alone (MCIT, 2024). The comparison therefore suggests that durable capability depends on the interaction of physical infrastructure with human capital, organisational learning, and domestic institutions. Megawatt scale may provide an enabling platform, but it does not automatically generate the capacity to modify systems, troubleshoot failures, develop complementary software, or negotiate effectively with suppliers.

Each stage of this conversion can nevertheless generate new dependence. More domestic data centres increase demand for imported processors; greater use of international cloud services can create reliance on proprietary software environments; workforce development around particular platforms can raise switching costs; and national AI companies can depend on foreign models, APIs, or development tools even when domestically owned. Resource-to-compute conversion therefore produces a progressively more complex ecosystem in which some vulnerabilities decline while others emerge.

This also explains why sovereign equity investment should not be equated with technological control. Gulf sovereign-fund investments can create commercial relationships, information advantages, and access to future opportunities, but they do not necessarily confer control over intellectual property, model architectures, semiconductor production, or corporate decisions. Financial ownership, physical localisation, operational control, intellectual-property ownership, and regulatory authority are distinct forms of power.

A practical implication concerns the regional balance between competition and cooperation. Saudi Arabia, the UAE, and Qatar compete for infrastructure, firms, investment, skills, research talent, and technological status, yet remain exposed to many of the same upstream suppliers and ecosystems. Selective cooperation in Arabic-language datasets, AI safety research, cybersecurity standards, model evaluation, professional training, interoperability, research infrastructure, and specialised applications could reduce duplication and expand the regional knowledge base. Such cooperation would not eliminate foreign dependence, but it could strengthen shared capacity to adapt, evaluate, and negotiate external technologies. The regional implication is therefore narrower than a call for technological integration. Cooperation is most plausible in areas where language, standards, evaluation, training, and shared research infrastructure can generate collective benefits without requiring states to surrender their distinct industrial strategies.

The three cases indicate that the transformation from hydrocarbon wealth to computational power is not a transition from dependence to independence but a reorganisation of dependence. Gulf states are gaining greater control over financing, infrastructure siting, data governance, deployment, and selected areas of model and institutional capability while remaining reliant on external actors for critical upstream technologies. This pattern is consistent with relational approaches to technological

interdependence, in which states can gain agency and bargaining power without controlling the network as a whole (Farrell & Newman, 2019; Roberts, 2024).

The strategic significance of current investment should therefore be assessed by what it produces beyond infrastructure. Planned megawatts, chip purchases, corporate investment, and sovereign funding matter insofar as they generate domestic expertise, institutional learning, software and model capability, supplier flexibility, cybersecurity resilience, and the ability to adapt when external conditions change. Localisation is a means rather than an endpoint: its value lies in whether it creates cumulative learning, substitution capacity, and bargaining power. Negotiated technological autonomy captures this condition—greater agency without full independence, and an effort to make unavoidable interdependence more manageable, resilient, and strategically useful.

11. CONCLUSION

Saudi Arabia, the UAE and Qatar are using resource-derived capital to build new forms of computational and institutional capacity. The comparison shows, however, that the transition from oil rent to compute power is not a movement from dependence to independence. It is better understood through resource-to-compute conversion and negotiated technological autonomy: states can deepen domestic capability and bargaining power while remaining embedded in foreign semiconductor, cloud, model, and regulatory ecosystems.

The article also shows why technological autonomy and governance autonomy should be distinguished. Physical localisation, domestic ownership, and sovereign investment do not by themselves determine who controls critical technological layers, while reliance on foreign technology does not eliminate domestic authority over data, cybersecurity, public-sector deployment, and ethical oversight. In the Gulf, these governance arrangements operate within Islamic constitutional environments but use a hybrid operational vocabulary that combines public-interest concerns with globally circulating principles of fairness, privacy, safety, transparency, accountability, and security.

The long-term significance of Gulf AI investment will therefore depend less on headline spending than on whether current projects generate locally embedded knowledge, research capacity, technical skills, interoperability, supplier flexibility, resilient infrastructure, and credible substitution options.

The central strategic question is not whether interdependence can be eliminated, but whether its terms can be shaped so that external dependence remains manageable while domestic institutions gain greater capacity to govern, adapt and negotiate advanced AI systems. In that sense, the shift from oil rent to compute power is a reconfiguration of state capacity, security and technological agency rather than the achievement of technological sovereignty.

References

- 1) Advanced Micro Devices. (2025, May 13). *AMD and HUMAIN form strategic, \$10B collaboration to advance global AI*. <https://newsroom.amd.com/news/amd-and-humain-form-strategic-10b-collaboration/>
- 2) Albous, M. R., Al-Jayyousi, O. R., & Stephens, M. (2025). AI governance in the GCC states: A comparative analysis of national AI strategies. *Journal of Artificial Intelligence Research*, 82, 2389–2422. <https://doi.org/10.1613/jair.1.17619>
- 3) Albous, M. R., Stephens, M., & Al-Jayyousi, O. R. (2025). Artificial intelligence and the Gulf Cooperation Council workforce: Adapting to the future of work. *Humanities and Social Sciences Communications*, 12, Article 1649. <https://doi.org/10.1057/s41599-025-05984-5>
- 4) Amiri Diwan. (2024, November 6). *HH the Amir ratifies 2024 constitutional amendments to Qatar's Permanent Constitution*. <https://diwan.gov.qa/en/briefing-room/legislations/2024/november/6/lq01>
- 5) Auda, J. (2008). *Maqasid al-Shariah as philosophy of Islamic law: A systems approach*. International Institute of Islamic Thought. <https://doi.org/10.2307/j.ctvkc67tg>
- 6) Basic Law of Governance, Royal Order No. A/90, arts. 1, 8 (1992). Bureau of Experts at the Council of Ministers. <https://laws.boe.gov.sa/Files/Download/?attId=ed4842e1-9543-40b9-973b-ada200d4ed10>
- 7) Blancato, F. G. (2024). The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem. *Policy & Internet*, 16, 12–32. <https://doi.org/10.1002/poi3.358>
- 8) Brown, N. J. (2002). *Constitutions in a nonconstitutional world: Arab basic laws and the prospects for accountable government*. State University of New York Press.
- 9) Constitution of the United Arab Emirates, art. 7 (1971). UAE Cabinet. <https://uaecabinet.ae/en/the-constitution>
- 10) Elmahjub, E. (2023). Artificial intelligence (AI) in Islamic ethics: Towards pluralist ethical benchmarking for AI. *Philosophy & Technology*, 36, Article 73. <https://doi.org/10.1007/s13347-023-00668-x>
- 11) 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
- 12) Korniyenko, Y., & Xin, W. (2025). *Gulf Cooperation Council diversification: The role of foreign investments and sovereign wealth funds* (IMF Working Paper 2025/174). International Monetary Fund. <https://doi.org/10.5089/9798229019514.001>
- 13) Lombardi, C. B. (2013). Constitutional provisions making Sharia “a” or “the” chief source of legislation: Where did they come from? What do they mean? Do they matter? *American University International Law Review*, 28(3), 733–774. <https://digitalcommons.law.uw.edu/faculty-articles/713/>
- 14) Microsoft. (2024, April 16). *Microsoft invests \$1.5 billion in Abu Dhabi's G42 to accelerate AI development and global expansion*. <https://news.microsoft.com/source/2024/04/16/microsoft-invests-1-5-billion-in-abu-dhabis-g42-to-accelerate-ai-development-and-global-expansion/>
- 15) Miller, R., & Wright, S. (2025). US-China AI competition in the Arab Gulf: Diverging uses of technological statecraft on the regional level. Alternatives: Global, Local, and Political. Advance online publication. <https://doi.org/10.1177/03043754251377866>
- 16) Ministry of Transport and Communications, State of Qatar. (2019). *National artificial intelligence strategy for Qatar*. https://www.mcit.gov.qa/wp-content/uploads/sites/4/2025/02/national_artificial_intelligence_strategy_for_qatar_2019_en.pdf

- 17) Ministry of Communications and Information Technology. (2024, May 16). *HE the Minister: We envision 'Fanar' as high-accuracy Arabic LLM capable of processing and understanding natural Arabic*. <https://www.mcit.gov.qa/en/news/he-the-minister-we-envision-fanar-as-high-accuracy-arabic-llm-capable-of-processing-and-understanding-natural-arabic/>
- 18) Ministry of Communications and Information Technology. (2025a, December 3). *MCIT signs a cooperation agreement with MEEZA to expand the Azure Qatar Data Center*. <https://www.mcit.gov.qa/en/news/mcit-signs-a-cooperation-agreement-with-meeza-to-expand-the-azure-qatar-data-center/>
- 19) Ministry of Communications and Information Technology. (2025b, February 25). *Ministry of Communications and Information Technology signs partnership initiative with Microsoft to launch Azure OpenAI Service to drive AI innovation from Qatar to the world*. <https://www.mcit.gov.qa/en/news/ministry-of-communications-and-information-technology-signs-partnership-initiative-with-microsoft-to-launch-azure-openai-service-to-drive-ai-innovation-from-qatar-to-the-world/>
- 20) Montambault Trudelle, A. (2024). Tools of regime stability: The political economy of sovereign wealth funds in Gulf rentier states. *Review of International Political Economy*, 31(5), 1446–1471. <https://doi.org/10.1080/09692290.2024.2325394>
- 21) NVIDIA. (2025, May 13). *HUMAIN and NVIDIA announce strategic partnership to build AI factories of the future in Saudi Arabia*. <https://nvidianews.nvidia.com/news/humain-and-nvidia-announce-strategic-partnership-to-build-ai-factories-of-the-future-in-saudi-arabia>
- 22) OpenAI. (2025, May 22). *Introducing Stargate UAE*. <https://openai.com/index/introducing-stargate-uae/>
- 23) Opwis, F. (2005). Maslaha in contemporary Islamic legal theory. *Islamic Law and Society*, 12(2), 182–223. <https://doi.org/10.1163/1568519054093699>
- 24) Ministry of Justice, State of Qatar. (2024). *the Permanent Constitution of the State of Qatar* (2nd Ed.). Government Communications Office. https://www.gco.gov.qa/wp-content/uploads/2024/12/permanent_constitution_state_qatar_en.pdf
- 25) 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/>
- 26) Qatar Investment Authority. (2025, December 9). *Brookfield and Qai form \$20 billion strategic investment partnership for AI infrastructure*. <https://www.qia.qa/en/Newsroom/Pages/Brookfield-and-Qai-Form-%2420-Billion-Strategic-Investment-Partnership-for-AI-Infrastructure.aspx>
- 27) Roberts, H. (2024). Digital sovereignty and artificial intelligence: A normative approach. *Ethics and Information Technology*, 26, Article 70. <https://doi.org/10.1007/s10676-024-09810-5>
- 28) Saudi Data & AI Authority. (2020). *National strategy for data & AI*. <https://sdaia.gov.sa/en/SDAIA/SdaiaStrategies/Pages/NationalStrategyForDataAndAI.aspx>
- 29) Saudi Data & AI Authority. (2023). *AI ethics principles*. <https://sdaia.gov.sa/en/SDAIA/about/Documents/ai-principles.pdf>
- 30) Seloom, M. (2026). Securitising AI: Routine exceptionality and digital governance in the Gulf. *AI and Ethics*, 6, Article 35. <https://doi.org/10.1007/s43681-025-00850-1>
- 31) Tran, E., & Gulrez, T. (2026). Polycentric power plays: Gulf agency and the dynamics of China's AI diplomacy. *Communication and the Public*. Advance online publication. <https://doi.org/10.1177/20570473261438564>

- 32) Minister of State for Artificial Intelligence, Digital Economy and Remote Work Applications Office. (2022). AI ethics: Principles & guidelines. <https://ai.gov.ae/wp-content/uploads/2023/05/MOCAI-AI-Ethics-EN.pdf>
- 33) Minister of State for Artificial Intelligence, Digital Economy and Remote Work Applications Office. (2024, July 30). The UAE Charter for the Development & Use of Artificial Intelligence. <https://ai.gov.ae/wp-content/uploads/2024/07/UAEAI-Methaq-EN2-3.pdf>
- 34) United Arab Emirates Government. (2017). *UAE strategy for artificial intelligence*. <https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/uae-strategy-for-artificial-intelligence>
- 35) United Arab Emirates Government. (2026). *The National Cyber Security Policy for Artificial Intelligence*. <https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/policies/cyber-activities/The-National-Cyber-Security-Policy-for-Artificial-Intelligence>
- 36) U.S. Department of Commerce. (2025a, November 19). *Statement on UAE and Saudi chip exports*. <https://www.commerce.gov/news/press-releases/2025/11/statement-uae-and-saudi-chip-exports>
- 37) U.S. Department of Commerce. (2025b, May 15). *UAE and US presidents attend the unveiling of Phase 1 of new 5GW AI campus in Abu Dhabi*. <https://www.commerce.gov/news/press-releases/2025/05/uae-and-us-presidents-attend-unveiling-phase-1-new-5gw-ai-campus-abu>
- 38) U.S. Department of Commerce. (2025c, May 15). *UAE/US framework on advanced technology cooperation*. <https://www.commerce.gov/news/press-releases/2025/05/uae/us-framework-advanced-technology-cooperation>