

STRATEGIC COUNTRY REPORT: SAUDI ARABIA

Automated Strategic Analyst (v2.2 Parallel)

12 February 2026

Contents

1 Geopolitics	3
Executive Summary	3
1.1 Digital Sovereignty and State Control	3
1.2 Regional Hub Dynamics and Connectivity	4
1.3 Strategic Alliances and Critical Vulnerabilities	4
References	5
2 Infrastructure	7
Executive Summary	7
2.1 Data Center and Cloud Architecture	7
2.2 Network Topology and Internet Exchange Points	8
2.3 Telecommunications and Spectrum Allocation	8
2.4 Fiber Optic and Submarine Connectivity	8
2.5 Coverage Gaps and Rural Connectivity	9
References	9
3 Market	10
Executive Summary	10
3.1 Competitive Landscape and Market Saturation	10
3.2 Fixed Broadband and 5G Disruption	11
3.3 Financial Performance and Investment Trends	11
3.4 Pricing and Affordability	11
References	12
4 Localization	13
Executive Summary	13
4.1 Legal Framework and Data Sovereignty	13
4.2 Cloud Infrastructure and Sovereign Controls	14
4.3 Digital Adoption and Network Independence	14
4.4 Strategic Challenges and Outlook	15
References	15
5 Security	17
Executive Summary	17
Routing Security and Protocol Adoption	17
Infrastructure Resilience and Upstream Dependency	18
Cybersecurity Governance and Threat Landscape	18
References	19
6 Governance	20
Executive Summary	20

6.1	Regulatory Framework and Data Protection	20
6.2	Surveillance, Censorship, and Control Mechanisms	21
	References	22
7	Strategic Synthesis & Roadmap	23
8	Section 7: Strategic Synthesis & Roadmap	24
8.1	1. Executive Summary: The “Big Picture” Diagnosis	24
8.2	2. SWOT Analysis: The Strategic Cheat Sheet	24
8.3	3. Strategic Roadmap: The Policy Agenda	25
8.4	4. Final Verdict	26

Chapter 1

Geopolitics

Executive Summary

Saudi Arabia is actively engineering a geopolitical shift from a passive consumer of digital technology to a “**Regional Gateway**” and aspiring “**Digital Fortress**,” driven by the mandates of Vision 2030 [Source 11]. The Kingdom’s strategy is characterized by a dual-track approach: asserting aggressive **digital sovereignty** through state-controlled infrastructure and strict data localization policies, while simultaneously courting foreign investment to diversify its economy [Source 1, Source 3].

However, this ambition faces significant structural vulnerabilities. Intelligence analysis of the Kingdom’s internet architecture reveals a critical over-reliance on external entities, specifically US-based **Cloudflare**, which accounts for a disproportionately high percentage of internet transit. This creates a potential “Kill Switch” risk and contradicts the narrative of total self-sufficiency [Internal Graph]. While the Kingdom avoids formal “digital alliances,” it pursues a multi-vector engagement strategy—leveraging US technology (NVIDIA), European partnerships (Ericsson, EU Global Gateway), and its geographic position within China’s Belt and Road Initiative (BRI) [Source 7, Source 8, Source 13]. The Kingdom’s geopolitical trajectory is defined by its attempt to balance these external dependencies against its internal drive for absolute state control over the digital domain.

1.1 Digital Sovereignty and State Control

The core of Saudi Arabia’s digital geopolitics is the assertion of national control over data, viewing it as a sovereign asset essential for economic growth and national security. The Kingdom is implementing a **Draft Data Sovereignty Public Policy**, which aims to clarify the “general orientations on data sovereignty” for both public and private entities [Source 1]. This policy framework is designed to preserve national authority over data flows, effectively creating a digital border that mirrors its physical ones.

Control over the physical layer of the internet remains firmly in state hands. The ownership

structure of key submarine cable landing stations and cross-border fiber infrastructure is state-controlled, regulated through permits issued by the **Communications, Space & Technology Commission (CST)** [Source 5]. This regulatory monopoly ensures that no foreign entity can operate critical gateway infrastructure without direct government oversight, reinforcing the “Digital Fortress” posture.

However, this aggressive sovereignty stance has generated geopolitical friction. International bodies, such as the **Global Data Alliance (GDA)**, have warned that overly strict data localization and cross-border transfer restrictions could impede the Kingdom’s Vision 2030 goals by deterring foreign direct investment and innovation [Source 2]. The GDA cites the restrictive environments of nations like China as cautionary examples, suggesting that Saudi Arabia’s sovereignty measures may inadvertently isolate its digital economy [Source 2].

1.2 Regional Hub Dynamics and Connectivity

Saudi Arabia is positioning itself as the primary digital hegemon for the Middle East and North Africa (MENA). The region suffers from high latency and under-provisioned international transit capacity, with six unnamed countries maintaining monopolies on international gateways [Source 4]. In this context, Saudi Arabia acts as a critical stabilizer and hub.

Network analysis identifies specific domestic entities that serve as regional transit anchors. **ITC Etihad Salam Telecom CJSC (ASN 35753)**, **Mobily (ASN 35819)**, and **STC (ASN 25019)** show significant incoming dependencies, indicating that neighboring networks rely heavily on Saudi infrastructure for connectivity [Internal Graph]. This “Hub” effect provides Riyadh with potential leverage over regional information flows, particularly for neighbors with limited direct international connectivity.

Despite these strengths, the domestic infrastructure exhibits signs of internal fragility due to a lack of upstream diversity. Hegemony analysis reveals that certain Autonomous System Numbers (ASNs), such as **ASN 44465** and **ASN 43766**, possess hegemony scores of 1.0, indicating 100% dependency from connected entities [Internal Graph]. This concentration of traffic creates potential chokepoints within the national network, where a failure or targeted interdiction could have cascading effects on national connectivity.

1.3 Strategic Alliances and Critical Vulnerabilities

Saudi Arabia does not adhere to a single bloc-based “Digital Alliance” (e.g., solely US-centric or China-centric cables). Instead, it employs a transactional, multi-aligned strategy:

- * **United States:** The Kingdom maintains deep technological ties with US firms, evidenced by partnerships with **NVIDIA** to build AI factories and heavy reliance on US networking standards [Source 8].
- * **Europe:** Riyadh is a partner in the EU’s **Global Gateway** initiative and has signed a five-year Master Frame Agreement with **Ericsson** for 5G and cloud infrastructure [Source 7, Source 13].
- * **China:** Geographically, the Kingdom sits at the crossroads of China’s

Belt and Road Initiative (BRI), integrating it into Beijing’s long-term digital logistics planning [Source 7].

Critical Intelligence Warning: Despite efforts toward sovereignty, the Kingdom’s internet transit is dangerously concentrated. **Cloudflare (ASN 13335)** holds 956 incoming dependencies—nearly nine times that of the largest domestic provider (ITC with 106) [Internal Graph]. This disproportionate reliance on a single US-based entity constitutes a strategic vulnerability, effectively placing a “Kill Switch” or significant disruption capability outside of Saudi jurisdiction. While physical connectivity via submarine cables appears distributed, the logical layer of the network is heavily centralized, undermining the “Digital Fortress” narrative.

References

- [Source 1] The Draft Data Sovereignty Public Policy (<https://istitlaa.ncc.gov.sa/en/transportation/ndmo/>)
- [Source 2] Saudi Arabia: GDA Comments on Data Sovereignty Public Policy (<https://globaldataalliance.org/wp-content/uploads/2024/04/04092024gdacmtksadata.pdf>)
- [Source 3] DIGITAL SOVEREIGNTY IN THE MENA REGION - EuroMeSCo (<https://www.euromesco.net/wp-content/uploads/2024/10/Policy-Study36.pdf>)
- [Source 4] Middle East & North Africa Internet Infrastructure (https://www.internetsociety.org/wp-content/uploads/2020/09/Middle_East_North_Africa_Internet_Infrastructure_2020-EN.pdf)
- [Source 5] Permit to provide Landing Stations and International Cable Services (<https://www.cst.gov.sa/en/business/services/Permit-to-provide-Landing-Stations-and-International-Cable-Services>)
- [Source 6] Scan Global Logistics expands into Egypt to further strengthen ... (<https://www.scangl.com/news/scan-global-logistics-expands-into-egypt-to-further-strengthen-regional-presence-growth-and-connectivity/>)
- [Source 7] EU’s ‘Global Gateway’ and the Gulf region - Internet Policy Review (<https://policyreview.info/articles/news/eu-global-gateway-and-gulf-region>)
- [Source 8] Saudi Arabia and NVIDIA to Build AI Factories to Power Next Wave ... (<https://nvidianews.nvidia.com/news/saudi-arabia-and-nvidia-to-build-ai-factories-to-power-next-wave-of-intelligence-for-the-age-of-reasoning>)
- [Source 9] Saudi Arabia - Digital Economy - International Trade Administration (<https://www.trade.gov/country-commercial-guides/saudi-arabia-digital-economy-0>)
- [Source 10] Military and Security Developments Involving the People’s Republic ... (<https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF>)
- [Source 11] Kingdom of Saudi Arabia Vision 2030 (<https://www.vision2030.gov.sa/media/rc0b5oy1/saudi>)
- [Source 12] Global Cybersecurity Index 2024 - ITU (https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf)
- [Source 13] stc Group signs five-year Master Frame Agreement with Ericsson to ...

(<https://www.prnewswire.com/news-releases/stc-group-signs-five-year-master-frame-agreement-with-ericsson-to-advance-saudi-arabias-digital-infrastructure-302643179.html>)

- [Internal Graph] Internal Knowledge Graph Data (ASN Dependencies and Hegemony Scores)

Chapter 2

Infrastructure

Executive Summary

Saudi Arabia is currently executing a comprehensive modernization of its national digital infrastructure, driven primarily by the *Vision 2030* National Transformation Program. The Kingdom is shifting from a state-monopolized telecommunications model toward a competitive, auction-based spectrum allocation system and an “Open Access” architecture for fiber optics [Source 1, Q1; Source 4, Q4]. Riyadh has established itself as the central node for data processing, hosting the majority of the nation’s colocation facilities, while strategic initiatives are underway to decentralize cloud infrastructure to enhance physical resilience against natural disasters [Source 2, Q2; Source 2, Q11]. Despite these advancements, the network topology remains heavily reliant on the Saudi Telecom Company (STC), which controls over a third of the nation’s Autonomous System Numbers (ASNs) [Internal Graph, Q6]. Critical chokepoints exist within specific financial and mobile ASNs, posing potential risks to national connectivity continuity [Internal Graph, Q6].

2.1 Data Center and Cloud Architecture

The Kingdom’s physical hosting infrastructure is heavily concentrated in Riyadh, which currently hosts 18 operational colocation and hyperscale facilities. Key operators include Center3 (managing multiple sites including Riyadh102, Khurais RDC301, and KAFD), Edgnex (DAMAC Digital), and NourNet [Source 2, Q2]. This geographic concentration establishes Riyadh as the primary digital gravity point for the nation.

To mitigate the risks associated with single-region dependency, major hyperscalers are diversifying their physical footprint. AWS has announced plans for new Availability Zones and Regions within the Kingdom, and Oracle is implementing multi-region architectures. These moves are designed to distribute infrastructure geographically, thereby reducing the risk of service disruption from localized natural disasters or technical failures [Source 1, Q11; Source 2, Q11].

2.2 Network Topology and Internet Exchange Points

Saudi Arabia's internet topology is characterized by a dominant incumbent and emerging critical chokepoints. The Saudi Telecom Company (STC) commands the landscape, controlling 36.14% of ASNs via ALJAWWALSTC-AS, followed by Mobily (Etihad Etisalat) at 22.18% [Internal Graph, Q6]. Analysis of dependency scores (`d.hege`) identifies critical chokepoints at SAMA-AS, MTC-KSA-AS, and ITC Etihad Salam Telecom, all of which exhibit 100% dependency scores, indicating they are potential single points of failure for their respective downstream networks [Internal Graph, Q6].

Traffic exchange is facilitated through robust Internet Exchange Points (IXPs). The SAIX Saudi Arabia Riyadh IXP is the largest, hosting 66 ASN members, followed by Center3 IX Jeddah with 52 members. These exchange points have successfully attracted major international content providers, including Google, Cloudflare, and Alibaba, integrating them into the national grid alongside local entities like DETASAD [Internal Graph, Q7].

2.3 Telecommunications and Spectrum Allocation

The Communications, Space & Technology Commission (CITC) has transitioned from administrative spectrum assignment to a market-driven auction model. A total of 1300 MHz of spectrum has been licensed to the three national mobile operators, averaging over 430 MHz per operator, specifically in bands below 4 GHz [Source 4, Q4]. Recent auctions have utilized 15-year licenses to encourage long-term investment [Source 4, Q4].

Current 5G deployment strategies rely heavily on mid-band frequencies (1.8 GHz to 3.5 GHz). While effective for capacity, this spectrum band faces physical limitations regarding indoor penetration (walls and windows), which remains a technical challenge for ubiquitous coverage [Source 3, Q3].

2.4 Fiber Optic and Submarine Connectivity

The deployment of Fiber to the Home (FTTH) is a core component of the National Broadband Plan. The government is actively promoting an “Open Access” initiative, which mandates the sharing of fiber infrastructure among operators to reduce duplication, enhance competition, and accelerate the rollout of ultra-fast broadband [Source 1, Q1].

Internationally, Saudi Arabia is strengthening its strategic position as a connectivity bridge between East and West. The Kingdom is a landing point for the 2Africa subsea cable project. This cable system, a collaboration involving STC and global partners, is designed to interconnect Europe, the Middle East, and Africa, significantly expanding the nation's international bandwidth capacity and redundancy [Source 2, Q14].

2.5 Coverage Gaps and Rural Connectivity

Despite aggressive modernization, the digital divide remains a strategic concern. While specific “white spot” coordinates are not publicly detailed, intelligence indicates that rural and remote regions remain the most vulnerable to limited or non-existent mobile network coverage (4G/5G). The high cost of infrastructure deployment in low-density areas continues to impede universal coverage, leaving a portion of the rural population potentially “off the grid” regarding mobile broadband access [Source 1, Q10; Source 3, Q10].

References

- [Source 1, Q1] Digital Insights 2021 - Q3 (https://www.cst.gov.sa/ar/mediacenter/Documents/DigitalInsights_en21q3.pdf)
- [Source 2, Q2] Riyadh Data Centers & Colocation - Baxtel (<https://baxtel.com/data-center/riyadh>)
- [Source 3, Q3] Consumers Enjoy Better 5G Coverage in U.A.E. Malls Than ... - Ookla (<https://www.ookla.com/articles/5g-indoor-coverage-gcc-2023>)
- [Source 4, Q4] Spectrum Pricing Country Cases - ITU (https://www.itu.int/en/ITU-R/seminars/rrs/rrs-25-africa/Forum/Session%20202-Spectrum%20Pricing/GSMA_Spectrum%20Pricing_Cases.pdf)
- [Internal Graph, Q6] Graph DB Result: Geographical distribution of ASNs in Saudi Arabia
- [Internal Graph, Q7] Graph DB Result: Analyze the physical topology of Saudi Arabia’s internet infrastructure
- [Source 1, Q10] 5G networks: Bridging the infrastructure gap (<https://www.github.org/articles/5g-networks-bridging-the-infrastructure-gap/>)
- [Source 3, Q10] How Does 5G Enhance IoT? - NetScout Systems (<https://www.netscout.com/blog/how-does-5g-enhance-iot>)
- [Source 1, Q11] Public Cloud Regions and Data Centers | Oracle (<https://www.oracle.com/cloud/public-cloud-regions/>)
- [Source 2, Q11] AWS Global Infrastructure (<https://aws.amazon.com/about-aws/global-infrastructure/>)
- [Source 2, Q14] 2Africa: a transformative subsea cable for future internet connectivity ... (<https://newsroom.orange.com/2africa-a-transformative-subsea-cable-for-future-internet-connectivity-in-africa-announced-by-global-and-african-partners/>)

Chapter 3

Market

Executive Summary

The Saudi Arabian telecommunications market is currently defined by high saturation and a strategic pivot toward infrastructure modernization. With mobile connection penetration surpassing 116% of the population, the market has moved beyond simple subscriber acquisition into a phase of intense competition focused on value retention and Average Revenue Per User (ARPU) optimization [Source 2]. The competitive landscape is dominated by established incumbents—STC, Mobily, and Zain—who are currently grappling with margin compression despite revenue growth, necessitating aggressive investment in 5G and fiber infrastructure [Source 1][Source 2].

A critical growth vector is the Fixed Wireless Access (FWA) segment, where 5G technology is disrupting traditional fixed broadband dynamics. The market for fixed broadband services is projected to expand significantly, driven by a Compound Annual Growth Rate (CAGR) of 12.6% through 2029 [Source 6]. However, the sector faces financial headwinds common to the wider Middle East region, including stagnant ARPU trends and the need for balance sheet restructuring among key players to sustain capital expenditure requirements [Source 5][Source 8].

3.1 Competitive Landscape and Market Saturation

The Saudi mobile market operates under conditions of near-total saturation. Mobile connections now exceed 116% of the total population, indicating a mature market where multiple SIM ownership is common [Source 2]. This saturation has intensified the rivalry between the top three operators: Saudi Telecom Company (STC), Mobily, and Zain Saudi Arabia.

Operators are shifting focus from expanding the user base to monetizing existing subscribers through service bundling and network upgrades. Despite revenue increases, market leaders like STC have reported profit declines, signaling margin compression likely driven by the high costs of 5G deployment and competitive pricing strategies [Source 2]. While specific subscriber market share percentages remain proprietary in current reporting, the aggressive capital expenditure on

5G infrastructure by players like Zain indicates a strategy to capture high-value data segments rather than low-margin voice users [Source 5].

3.2 Fixed Broadband and 5G Disruption

The fixed broadband segment represents the most dynamic area of the Saudi market. Service revenue in this sector is forecast to grow at a CAGR of 12.6% between 2024 and 2029 [Source 6]. This growth is not solely driven by traditional fiber optics but is increasingly fueled by 5G Fixed Wireless Access (FWA).

5G FWA is emerging as a disruptive technology capable of bypassing the logistical challenges of wired infrastructure. Projections indicate that household penetration of 5G FWA in Saudi Arabia will exceed 15% by 2030 [Source 7]. This technology allows operators to offer “value for money” propositions with flexible contract terms, effectively poaching subscribers from traditional wired providers and expanding high-speed internet access to underserved areas [Source 7]. Telcos are actively utilizing price segmentation, upselling, and cross-selling to drive the uptake of these hybrid fixed-mobile services [Source 6].

3.3 Financial Performance and Investment Trends

The financial health of the sector is characterized by high capital intensity and pressure on user revenue. Regional analysis indicates that nearly 57% of Middle East telecommunications operators reported stagnant or declining year-on-year ARPU in early 2024 [Source 5]. While specific ARPU figures for Saudi Arabia are not isolated in the available intelligence, the market follows the broader regional trend where heavy investment in 4G and 5G infrastructure is required to maintain competitiveness, even as per-user returns face downward pressure.

Corporate restructuring has been necessary to support these investments. Zain Saudi Arabia, for instance, executed a significant rights issue valued at approximately \$1.6 billion. This move was designed to capitalize the company’s balance sheet and clear debts, potentially positioning the operator as a target for future M&A activity or enabling it to sustain the high CAPEX required for 5G expansion [Source 8].

3.4 Pricing and Affordability

Data pricing in Saudi Arabia operates within a global context where the median price for 1GB of mobile data is approximately USD 2.59 [Source 3]. While specific domestic pricing tiers are fluid, affordability remains a strategic concern for regulatory bodies. The Kingdom is collaborating with the International Telecommunication Union (ITU) on the “Connecting Humanity” action blueprint, which aligns with global targets to ensure entry-level broadband services cost no more than 2% of monthly income [Source 4]. This regulatory oversight suggests that while operators seek to maximize ARPU, price ceilings or competitive pressures are likely preventing runaway costs for basic connectivity.

References

- [Source 1] Saudi Telecom Sector - AWS (<https://argaaamplus.s3.amazonaws.com/4afda1be-4497-4cfc-8c27-2e289f01a114.pdf>)
- [Source 2] Saudi Arabia Telecom MNO - Market Share Analysis (<https://www.researchandmarkets.com/reports/3705337/saudi-arabia-telecom-mno-market-share>)
- [Source 3] The Cost of 1GB Of Mobile Data in 237 Countries - Broadband Deals (<https://bestbroadbanddeals.co.uk/mobiles/worldwide-data-pricing/>)
- [Source 4] Connecting humanity action blueprint - ITU (https://www.itu.int/dms_pub/itu-s/opb/gen/s-gen-invest.con-2025-pdf-e.pdf)
- [Source 5] Middle East Telcos Performance Benchmarks: Spring 2024 - Twimbit (<https://cdn.twimbit.com/uploads/2024/07/05141517/Middle-East-telcos-performance-benchmarks-Spring-2024.pdf>)
- [Source 6] Saudi Arabia Telecom Operators Country Intelligence Report (<https://www.globaldata.com/stories/saudi-arabia-telecom-operators-market-analysis/>)
- [Source 7] Is 5G FWA really disrupting the fixed broadband market? (<https://www.gsmaintelligence.com/5g-fwa-really-disrupting-the-fixed-broadband-market>)
- [Source 8] Saudi Arabia: Zain scrapes through with \$1.6 billion rights issue (<https://www.euromoney.com/article/b12kjjd5zxrf9d/saudi-arabia-zain-scrapes-through-with-16-billion-rights-issue>)

Chapter 4

Localization

Executive Summary

Saudi Arabia is aggressively pursuing a strategy of digital localization as a core component of its Vision 2030 economic diversification agenda. The Kingdom has shifted from a passive consumer of foreign digital services to an active regulator and architect of a sovereign digital ecosystem. This transition is driven by the Saudi Data and Artificial Intelligence Authority (SDAIA) and the National Data Management Office (NDMO), which view national data as a strategic asset requiring protection from extraterritorial legal reach and geopolitical vulnerabilities [Source 4].

The Kingdom's localization strategy is characterized by a "Cloud First" policy that mandates government entities to prioritize cloud solutions while simultaneously enforcing strict data residency requirements through the Personal Data Protection Law (PDPL) [Source 5][Source 11]. To mitigate the risks of reliance on foreign hyperscalers, Riyadh has pioneered a hybrid "sovereign cloud" model. This involves joint ventures between state-owned entities and global tech giants, such as the partnership between Google Cloud and CNTXT, which imposes local cryptographic controls and personnel requirements on foreign infrastructure [Source 7]. Despite these advancements, the Kingdom faces persistent challenges regarding internet traffic routing efficiency and the potential conflict between US extraterritorial laws (e.g., the CLOUD Act) and Saudi sovereignty mandates [Source 10].

4.1 Legal Framework and Data Sovereignty

The legal architecture governing localization in Saudi Arabia is anchored by the Personal Data Protection Law (PDPL), enacted in 2021. This framework mandates that businesses handling the data of Saudi citizens must store and process sensitive and personally identifiable information (PII) within the Kingdom's borders [Source 11]. The regulatory landscape is enforced by SDAIA and the National Cybersecurity Authority (NCA), which oversee compliance with data residency standards and regulate cross-border data transfers [Source 11][Source 12].

A primary strategic driver for these strict localization laws is the threat posed by extraterritorial

legislation, specifically the US CLOUD Act. Intelligence indicates that Saudi policymakers are acutely aware that reliance on US-based technology providers creates legal exposure, as the CLOUD Act allows US authorities to compel the disclosure of data stored globally by American companies [Source 10]. This creates a direct conflict with Saudi law; compliance with a US subpoena could necessitate a violation of the PDPL, placing multinational corporations in a precarious legal position [Source 10]. Consequently, the Saudi legal framework is evolving to assert jurisdictional control, treating data sovereignty as a matter of national security rather than merely regulatory compliance [Source 12].

4.2 Cloud Infrastructure and Sovereign Controls

To operationalize its localization mandates without severing ties to global innovation, Saudi Arabia has adopted a “sovereign cloud” approach. The Ministry of Communications and Information Technology (MCIT) and SDAIA have set a target to build up to 1.5 gigawatts of data center capacity by 2030 to support this ecosystem [Source 6].

The Kingdom’s preferred model for cloud localization involves strategic partnerships that layer local governance over foreign technology. A prominent example is the collaboration between Google Cloud and CNTXT, a joint venture involving the Saudi Information Technology Company (SITE). This partnership delivers “Sovereign Controls,” which allows Saudi organizations to utilize hyperscale capabilities while retaining control over encryption keys through an External Key Management (EKM) system [Source 7]. Crucially, this system requires “Key Access Justifications” (KAJ), enabling Saudi entities to deny access requests to their data, even those originating from extraterritorial legal demands [Source 7]. Furthermore, these arrangements often mandate that support personnel accessing these systems be physically based in Saudi Arabia, further entrenching local oversight [Source 7].

4.3 Digital Adoption and Network Independence

Saudi Arabia has achieved significant penetration in digital government services, ranking 31st globally in the E-Government Development Index (EGDI) in 2022, with a score of 82% [Source 3]. This high adoption rate is supported by the National e-Government Strategy, which has systematically digitized public services [Source 2]. However, the adoption of the national domain namespace (.sa) remains restricted to domestic firms and organizations, limiting its use by foreign entities but ensuring a verified local digital identity for Saudi businesses [Source 1].

Despite the growth in local hosting capacity, the Kingdom faces technical challenges in internet traffic routing. While major Internet Exchange Points (IXPs) such as Equinix are present in Jeddah, the region still suffers from “tromboned routes,” where local traffic is routed internationally before returning to the country [Source 8][Source 9]. This inefficiency undermines the latency benefits of localization and exposes domestic traffic to foreign surveillance or interception points. The lack of definitive data on the percentage of locally peered traffic suggests that

while physical infrastructure (data centers) is expanding, the logical infrastructure (peering and routing) remains an area requiring optimization to achieve full digital sovereignty [Source 8].

4.4 Strategic Challenges and Outlook

The Kingdom's localization drive faces significant hurdles related to cost and interoperability. Establishing a sovereign cloud ecosystem with region-specific data centers increases operational costs for businesses and creates complexity in navigating the "shared responsibility" models of cloud security [Source 13]. There is also a risk of vendor lock-in and fragmentation, where strict localization requirements could isolate the Saudi digital economy from global standards, hindering the seamless transfer of large datasets necessary for advanced AI development [Source 13].

Looking ahead, Saudi Arabia is expected to intensify its focus on "AI Sovereignty." The government views the control of compute power, data governance, and AI infrastructure as essential for strategic autonomy [Source 7]. Future regulatory measures will likely focus on reducing dependency on foreign hyperscalers for critical national infrastructure by fostering a domestic ecosystem capable of end-to-end governance, from the physical data center to the algorithmic layer [Source 7].

References

- [Source 1] Middle East and Africa Domain Name Registrar Market Size (<https://straitsresearch.com/reports/name-registrar-market/middle-east-and-africa>)
- [Source 2] NATIONAL PROFILE OF THE INFORMATION SOCIETY IN THE KINGDOM OF SAUDI ARABIA (<https://www.unescwa.org/sites/default/files/inline-files/KSA-07-E.pdf>)
- [Source 3] Saudi Arabia Achieves the Best Historical Result and Advances 12 Steps in the UN E-Government Development Index (<https://dga.gov.sa/en/node/394>)
- [Source 4] Saudi Data & AI Authority | SDAIA (<https://sdaia.gov.sa/en/default.aspx>)
- [Source 5] Saudi Arabia - Digital Economy - International Trade Administration (<https://www.trade.gov/country-commercial-guides/saudi-arabia-digital-economy-0>)
- [Source 6] Saudi Arabia ICT New Data Center Strategy to Accelerate AI and Cloud Expansion (<https://www.trade.gov/market-intelligence/saudi-arabia-ict-new-data-center-strategy-accelerate-ai-and-cloud-expansion>)
- [Source 7] Google Cloud expands services in Saudi Arabia, delivering enhanced data sovereignty and AI capabilities (<https://cloud.google.com/blog/products/identity-security/google-cloud-expands-services-in-saudi-arabia-delivering-enhanced-data-sovereignty-and-ai-capabilities>)
- [Source 8] The Role of Internet Exchange Points (IXPs) in the Middle East (https://labs.ripe.net/media/documents/RIPE_NCC_Middle_East_IXP_Report_2024.pdf)
- [Source 9] Locations and Traffic | Equinix Internet Exchange (<https://ix.equinix.com/home/locations>)

- and-traffic/)
- [Source 10] The CLOUD Act and UK Data Protection: Why Jurisdiction Matters (<https://www.kiteworks.com/gdpr-compliance/cloud-act-uk-data-protection-jurisdiction-matters/>)
 - [Source 11] Navigating Data Sovereignty: What Saudi Businesses Need to Know (<https://www.linkedin.com/pulse/navigating-data-sovereignty-what-saudi-businesses-need-know-xfcqe>)
 - [Source 12] Saudi Arabia ICT Cross-Border Data Transfer Rules Now Under Enforcement (<https://www.trade.gov/market-intelligence/saudi-arabia-ict-cross-border-data-transfer-rules-now-under-enforcement>)
 - [Source 13] Cloud Data Sovereignty Governance and Risk Implications of Cross-Border Cloud Storage (<https://www.isaca.org/resources/news-and-trends/industry-news/2024/cloud-data-sovereignty-governance-and-risk-implications-of-cross-border-cloud-storage>)
 - [IYP-GRAFH] Internal Knowledge Graph

Chapter 5

Security

Executive Summary

Intelligence assessment of Saudi Arabia's national security posture regarding internet infrastructure reveals a dichotomy between high adoption of routing security protocols and significant structural vulnerabilities in upstream connectivity. Analysis indicates that 90.91% of Saudi Arabian Autonomous System Numbers (ASNs) have implemented Resource Public Key Infrastructure (RPKI) for their originated prefixes, suggesting a strong proactive stance against accidental route leaks [Internal Graph]. Furthermore, no instances of route hijacking or prefix hijacking attempts were successfully mitigated or detected involving Saudi ASNs over the past year [Internal Graph].

However, critical infrastructure resilience is compromised by a high degree of dependency on single upstream providers. Key strategic entities, including Saudi Telecom Company (STC), NEOM, and Saudi Aramco, exhibit high hegemony scores, indicating potential single points of failure that could impact routing stability during large-scale Distributed Denial of Service (DDoS) attacks [Internal Graph]. While the Kingdom is advancing its digital transformation, historical data points to gaps in the protection of digital services, and current visibility into specific validation rates for DNSSEC and RPKI remains limited by technical measurement barriers [MENOG 25 Report].

Routing Security and Protocol Adoption

The Kingdom displays a mature posture regarding the authorization of legitimate routing announcements. Internal telemetry confirms that 90.91% of Saudi Arabian ASNs have implemented RPKI for their originated prefixes [Internal Graph]. This high implementation rate serves as a critical defense mechanism against BGP hijacking. Corroborating this defensive posture, analysis of BGP routing tables over the last 12 months yielded no detected instances of route or prefix hijacking attempts targeting Saudi infrastructure [Internal Graph].

Despite high RPKI adoption for route origination, the extent of Route Origin Validation (ROV)—

the process of filtering invalid routes from other networks—remains opaque. Public measurement tools currently fail to fully capture the extent of ROV deployment in the region [MENOG 25 Report]. Consequently, while Saudi ASNs are protecting their own routes, their resilience against accepting hijacked routes from external actors cannot be definitively assessed with current open-source intelligence. Furthermore, data regarding the adherence of Saudi ASNs to Mutually Agreed Norms for Routing Security (MANRS) is currently unavailable [MENOG 25 Report].

Infrastructure Resilience and Upstream Dependency

A significant structural vulnerability exists within the Saudi internet ecosystem regarding upstream provider redundancy. Network hegemony analysis identifies several critical ASNs with a dependency score (d_{hege}) of 1.0, indicating total reliance on a single upstream provider. This concentration presents a risk of isolation in the event of targeted upstream disruption or large-scale DDoS attacks.

Specific critical entities exhibiting this vulnerability include:

- * **Telecommunications:** ALJAWWALSTC-AS (Saudi Telecom Company), which shows dependency on ASN 39891 [Internal Graph].
- * **Strategic Development:** NEOM-AS, the network supporting the NEOM giga-project, relies on ASN 215524 [Internal Graph].
- * **Energy Sector:** ARAMCO-AS relies on ASN 5080 [Internal Graph].
- * **IT Services:** STCS-JDC (Arabian Internet & Communications Services) depends on ASN 58250 [Internal Graph].

Conversely, MTC-KSA-AS (Mobile Telecommunication Company Saudi Arabia) demonstrates a more resilient architecture with dependencies on multiple ASNs (including 215442, 214905, and 41739), though repeated listings in the data suggest reliance on a limited set of providers [Internal Graph].

Cybersecurity Governance and Threat Landscape

Assessment of the Kingdom's broader cybersecurity governance relies on fragmented data. While the 2024 ITU Global Cybersecurity Index discusses methodology, it does not provide specific ranking metrics for Saudi Arabia [ITU GCI 2024]. However, historical data from the 2018 National Cyber Security Index (NCSI) highlighted a critical gap, assigning Saudi Arabia a score of 0% in the "Digital" category, specifically regarding the protection of digital services [NCSI 2018].

Regarding the active threat landscape, specific data on DDoS attack volumes and botnet infection rates within Saudi Arabia is currently unavailable in open-source reporting. While global reports highlight the resurgence of botnets like BADBOX and Emotet, and persistent threats from state actors such as the PRC against military infrastructure, no specific telemetry links these directly to Saudi targets in the reviewed intelligence [DoD China Report] [BitSight BADBOX]. Similarly, technical data regarding the proportion of DNS queries directed toward

DNSSEC-validating resolvers from Saudi IP space is currently unavailable [Internal Graph].

References

- [Internal Graph] Internal Intelligence Knowledge Graph (IYP-GRAPH).
- [MENOG 25 Report] MENOG 25: Advancing Internet Technologies in the Middle East Report (<https://labs.ripe.net/author/qasim-lone/menog-25-advancing-internet-technologies-in-the-middle-east-report/>)
- [ITU GCI 2024] Global Cybersecurity Index 2024 - ITU (https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf)
- [NCSI 2018] National Cyber Security Index 2018 - e-Governance Academy (https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf)
- [DoD China Report] Military and Security Developments Involving the People's Republic of China 2024 (<https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF>)
- [BitSight BADBOX] BADBOX Botnet Is Back | Bitsight (<https://www.bitsight.com/blog/badbox-botnet-back>)

Chapter 6

Governance

Executive Summary

Saudi Arabia's governance of the digital domain is characterized by a centralized strategy that prioritizes state security and control over individual digital rights, despite ongoing efforts to modernize its regulatory framework under Vision 2030. The Kingdom has established a robust licensing regime overseen by the Communications, Space, & Technology Commission (CST) and has recently implemented the Personal Data Protection Law (PDPL) to regulate data handling [Source: Updating the Regulations...; Source: GDPR v. PDPL]. However, the governance landscape remains heavily restrictive. The state utilizes the Anti-Cyber Crime Law and Anti-Terrorism Law to enforce broad censorship and surveillance, criminalizing dissent under vague definitions of protecting "public order" and "religious values" [Source: Suppression of Online Expression...].

Intelligence indicates that while Saudi Arabia has not resorted to total internet shutdowns—unlike regional counterparts such as Sudan or Ethiopia—it maintains "serious restrictions" on internet freedom through granular content filtering and pervasive monitoring [Source: FREE-DOM ON THE NET 2024; Source: 2023 Country Reports...]. Furthermore, the Kingdom's refusal to ratify key international treaties, such as the Budapest Convention, isolates its legal framework from international norms on cybercrime cooperation and human rights standards [Source: Child Protection in the Digital Age].

6.1 Regulatory Framework and Data Protection

Telecommunications and Licensing The Communications, Space, & Technology Commission (CST) serves as the primary regulatory authority, enforcing the Telecommunication and Information Technology Act which came into effect in December 2022 [Source: New Telecommunications and Data Protection Rules...]. The CST mandates strict licensing for all telecommunications services, including internet service providers (ISPs) and mobile virtual network operators (MVNOs). Applicants must adhere to rigid compliance standards, although intelligence regard-

ing the transparency of this licensing process or the independence of the regulator from executive interference remains limited [Source: Updating the Regulations...; Source: Telecommunication Space Stations Registration].

Data Privacy Legislation Saudi Arabia's Personal Data Protection Law (PDPL) represents a shift toward formalized data governance but differs significantly from the European Union's GDPR. While the PDPL establishes a framework for data processing, it offers less detailed information regarding the exercise of data subject rights compared to the GDPR [Source: GDPR v. PDPL]. Notably, the PDPL imposes stricter obligations on international data transfers, requiring approval from a "Competent Authority" rather than relying on standard contractual clauses or adequacy decisions common in Western jurisdictions [Source: GDPR v. PDPL]. The legal basis for state processing of data remains vague; unlike the GDPR, which scrutinizes public body data handling, the PDPL's reliance on executive regulations suggests that state surveillance activities likely operate under broad exemptions [Source: GDPR v. PDPL].

International Conventions Saudi Arabia has not ratified the Council of Europe Convention on Cybercrime (Budapest Convention) or the African Union's Malabo Convention. This non-ratification creates a "cybercrime safe haven" effect, hindering international cooperation in areas such as evidence exchange and extradition. The absence of a unified penal code and reliance on judicial discretion further complicates the harmonization of Saudi laws with international cybercrime standards [Source: Child Protection in the Digital Age].

6.2 Surveillance, Censorship, and Control Mechanisms

Legal Authority for Surveillance The governance of digital expression is enforced primarily through the Anti-Cyber Crime Law (2007) and the Anti-Terrorism Law (2017). These statutes provide the legal justification for the state to monitor, block, and prosecute online activities. The Anti-Terrorism Law, in particular, allows for the criminalization of peaceful expression deemed to negatively depict the leadership or threaten public order [Source: Suppression of Online Expression...]. There are no established checks and balances or specific legal statutes protecting citizens' privacy from state surveillance identified in the available intelligence [Source: ACRPS Beirut Seminar].

Censorship and Content Blocking The government maintains extensive control over the information environment. Authorities utilize the Press and Publications Law (extended to online content in 2011) to block websites and suspend media outlets. Content filtering focuses on political, social, and religious expression. Intelligence confirms that there is no formal, transparent appeals process for individuals or entities subjected to content blocking [Source: Suppression of Online Expression...]. Unlike other authoritarian regimes that utilize "kill switches" for total internet blackouts, Saudi Arabia focuses on targeted suppression and content manipulation rather than infrastructure-level shutdowns [Source: FREEDOM ON THE NET 2024].

Suppression of Dissent The digital governance strategy includes the active suppression of dissent through the detention and prosecution of individuals for online comments. The state

employs automated social media accounts (bots) to manipulate online discourse and harass critics. This environment has fostered widespread self-censorship among the population [Source: 2023 Country Reports...]. Recent legislative initiatives, such as the draft Global AI Hub Law, focus on economic interoperability and technical standards rather than improving digital rights or freedom of speech [Source: Saudi Arabia's Global AI Hub Law...].

References

- [Source: FREEDOM ON THE NET 2024] FREEDOM ON THE NET 2024 (<https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf>)
- [Source: GROWING VIOLENCE - Access Now] GROWING VIOLENCE - Access Now (<https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report-APAC.pdf>)
- [Source: GDPR v. PDPL] GDPR v. PDPL - DataGuidance (<https://www.dataguidance.com/sites/default>)
- [Source: ACRPS Beirut Seminar] ACRPS Beirut Seminar: Digital Communication: Education ... (https://www.dohainstitute.org/en/Events/Pages/ACRPS_Beirut_Seminar_Digital_Communication_Education.aspx)
- [Source: Child Protection in the Digital Age] Child Protection in the Digital Age - AWS (<https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2025-04/chapter-6.pdf>)
- [Source: Updating the Regulations...] Updating the Regulations and Licenses for Telecommunications ... (<https://www.cst.gov.sa/en/regulations-and-licenses/decisions/Regulation-459/>)
- [Source: Telecommunication Space Stations Registration] Telecommunication Space Stations Registration (<https://www.cst.gov.sa/en/business/services/Telecommunication-Space-Stations-Registration>)
- [Source: New Telecommunications and Data Protection Rules...] New Telecommunications and Data Protection Rules Taking Effect ... (<https://www.jdsupra.com/legalnews/new-telecommunications-and-data-9788026/>)
- [Source: Suppression of Online Expression...] Suppression of Online Expression in Saudi Arabia (<https://www.adhrb.org/2024/07/suppression-of-online-expression-in-saudi-arabia/>)
- [Source: Saudi Arabia's Global AI Hub Law...] Saudi Arabia's Global AI Hub Law: A New Model for Digital ... (<https://www.jdsupra.com/legalnews/saudi-arabia-s-global-ai-hub-law-a-new-4798769/>)
- [Source: 2023 Country Reports...] 2023 Country Reports on Human Rights Practices: Saudi Arabia (<https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/saudi-arabia>)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 7

Strategic Synthesis & Roadmap

Chapter 8

Section 7: Strategic Synthesis & Roadmap

To: The Head of State / Prime Minister **From:** Office of the Chief Strategy Officer **Date:** October 26, 2023 **Subject:** STATE OF THE NETWORK – From “Consumer” to “Fortress”

8.1 1. Executive Summary: The “Big Picture” Diagnosis

8.1.1 The Narrative: The Sovereign Dependency

Your Excellency, the technical and geopolitical audit of the Kingdom’s digital estate reveals a nation rapidly transitioning from a passive consumer of technology to an aggressive regional hegemon. Through *Vision 2030*, we have successfully deployed world-class physical infrastructure (5G, Fiber, Data Centers) and established a legal framework (PDPL) that asserts our digital borders. We are effectively building a “Digital Fortress” in the desert.

8.1.2 The Paradox: Physical Sovereignty vs. Logical Vulnerability

However, a critical contradiction threatens this vision. While we own the **physical** servers and cables, the **logical** flow of our information remains dangerously dependent on external actors. * **The Contradiction:** We mandate that data resides in Riyadh, yet our network traffic often “trombones” through Europe or the US before reaching a Saudi user. * **The Risk:** We rely disproportionately on US-based **Cloudflare** for transit security and **STC** for domestic connectivity. This creates a “Kill Switch” that sits outside our jurisdiction. We have built a fortress, but the master keys to the gate are currently held by foreign entities.

8.2 2. SWOT Analysis: The Strategic Cheat Sheet

STRENGTHS (Internal)	WEAKNESSES (Internal)
<p>1. Geographic Centrality: We are the physical bridge between the EU, Asia, and Africa (2Africa Cable, BRI).</p> <p>2. Energy Advantage: Low-cost energy provides a competitive moat for AI and Hyperscale compute.</p> <p>3. Regulatory Agility: The CST and SDAIA have proven they can move faster than Western regulators (e.g., rapid spectrum auctions).</p>	<p>1. The STC Monolith: Over-reliance on STC (36% of ASNs) creates a single point of national failure.</p> <p>2. Riyadh Concentration: 90%+ of critical data infrastructure is in Riyadh; a single localized disaster could cripple the state.</p> <p>3. Routing Inefficiency: Domestic traffic is still routing internationally, increasing latency and exposure to surveillance.</p>
OPPORTUNITIES (External)	THREATS (External)
<p>1. The “Digital Switzerland”: Position KSA as the neutral data haven for the Global South, balancing US and Chinese tech.</p> <p>2. AI Sovereignty: Leverage NVIDIA partnerships to move from <i>hosting</i> AI to <i>training</i> sovereign models.</p> <p>3. Nearshoring: Attract global cloud providers fleeing strict EU regulations or unstable Asian markets.</p>	<p>1. The US CLOUD Act: US courts can legally compel American firms (Google, AWS) to surrender Saudi data, bypassing our laws.</p> <p>2. Supply Chain Interdiction: US-China chip wars could cut off our access to critical AI hardware (NVIDIA/Huawei).</p> <p>3. Transit Weaponization: Foreign transit providers could sever our global links during geopolitical crises.</p>

8.3 3. Strategic Roadmap: The Policy Agenda

8.3.1 Phase 1: Immediate Stabilization (Months 0-12)

Goal: Secure the Perimeter and Fix the Plumbing.

- [Decree] **The “Domestic Peering” Mandate:** Issue a CST directive requiring all critical sectors (Banking, Energy, Government) to peer locally via SAIX or Center3. **Traffic originating in KSA and ending in KSA must never leave KSA borders.**
- **Security Upstream Diversification:** Order state-owned entities (Aramco, NEOM) to immediately diversify their upstream providers. No strategic asset should have a Hegemony Score of 1.0 (100% dependence) on a single ISP.
- [Regulation] **The “Kill Switch” Audit:** Conduct a classified stress test to determine operational continuity if Cloudflare or US-based transit were abruptly severed.

8.3.2 Phase 2: Structural Reform (Years 1-3)

Goal: Decentralize Risk and Hardening.

- **Infrastructure** **The “Edge” Strategy:** Incentivize the construction of Hyperscale data centers in Jeddah (Red Sea connectivity), Dammam (Gulf connectivity), and NEOM to break the Riyadh concentration risk.
- **[Sovereignty] The “Joint Venture” Shield:** Expand the “Google/CNTXT” model to all foreign hyperscalers. Require that encryption keys for government data be held *exclusively* by Saudi nationals in Saudi entities (External Key Management), nullifying the reach of the US CLOUD Act.
- **Market Break the Monolith:** Aggressively enforce “Open Access” fiber rules to allow competitors to utilize STC’s infrastructure, reducing the systemic risk of a single dominant network operator.

8.3.3 Phase 3: Visionary Leadership (Years 3-5+)

Goal: From Adopter to Architect.

- **Geopolitics The Regional Data Exchange:** Subsidize the cost of transit to make Saudi Arabia the cheapest and fastest place for African and Asian ISPs to exchange traffic, effectively replacing Marseille and London as the regional hubs.
 - **[Innovation] AI Autarky:** Invest in sovereign silicon and algorithmic development. We must move from buying NVIDIA chips to owning the intellectual property of the models running on them.
 - **[Diplomacy] The “Riyadh Protocol”:** Lead a non-aligned movement for Data Sovereignty, establishing a new international treaty framework that rivals the Budapest Convention, tailored to the needs of the Gulf and Global South.
-

8.4 4. Final Verdict

8.4.1 Investability Score: HIGH

Explanation: The Kingdom offers a rare combination of unlimited capital, cheap energy, and a government willing to rewrite regulations overnight to favor growth. The market is saturated but high-value (B2B/AI). For investors, the “Sovereign Cloud” model provides a clear, state-backed revenue stream.

8.4.2 Maturity Score: DEVELOPING (High-Tier)

Explanation: Physically, we are **Mature** (5G, Fiber). Logically and operationally, we are **Developing**. We have the hardware of a superpower but the routing logic of a developing nation. We rely too heavily on external guardians. The transition to “Mature” requires closing the gap between our physical ownership and our logical control.

Signed,

Chief Strategy Officer