STRATEGIC COUNTRY REPORT: UNITED ARAB EMIRATES

Automated Strategic Analyst (v2.2 Parallel)

12 February 2026

Contents

Chapter 1

Geopolitics

Executive Summary

The United Arab Emirates (UAE) is executing a high-stakes geopolitical strategy of "digital non-alignment," positioning itself as a critical node between the Chinese Digital Silk Road (DSR) and Western technology ecosystems. The nation actively balances partnerships with US-based hyperscalers (AWS, Google, Microsoft) against deep integration with Chinese infrastructure providers like Huawei and Alibaba, aiming to maximize economic diversification and technological transfer [Source 1]. This balancing act is underpinned by a robust "National Sovereign Cloud" strategy designed to mitigate the legal reach of foreign powers, specifically the U.S. CLOUD Act, and to secure data for national AI superiority [Source 4].

Despite these strategic ambitions, technical intelligence reveals significant vulnerabilities in the UAE's critical internet infrastructure. While the state maintains strict ownership over landing stations via Etisalat [Source 3], the national network topology exhibits high centralization and fragility rather than resilience [IYP-GRAPH]. Furthermore, key state-owned operators (Etisalat and Du) have failed to adopt critical BGP security standards (RPKI ROV), leaving the national grid susceptible to external routing manipulation, in stark contrast to the secure posture of foreign entities operating within the country [IYP-GRAPH].

1.1 Strategic Positioning and Digital Alliances

The UAE's digital geopolitics are defined by its role as a "crossroads" for global infrastructure, effectively leveraging its geography to engage competing global powers.

The East-West Balancing Act The UAE has integrated itself into China's Belt and Road Initiative (BRI), serving as a connecting point for the Digital Silk Road between China and Europe [Source 2]. This alignment facilitates the entry of Chinese tech giants; Alibaba and Tencent are expanding cloud operations, and Huawei is instrumental in the nation's broadband and public cloud services [Source 1]. Simultaneously, the UAE remains a primary hub for Western investment. US technology firms, including Amazon Web Services (AWS), Google, and

Microsoft, have established significant cloud regions in the country to capture the MENA market [Source 1]. This dual-engagement strategy allows the UAE to avoid strict geopolitical alignment while fostering intense competition for its domestic cloud market.

Regional and European Integration Beyond the US-China dynamic, the UAE is diversifying its connectivity through the European Union's "Global Gateway" initiative and strategic partnerships with the Gulf Cooperation Council (GCC). These alliances focus on the data economy and AI cooperation [Source 2]. Recent commercial engagements, such as discussions with 4iG Nyrt to expand a subsea digital backbone across the Mediterranean, indicate a strategic push to solidify connectivity with Europe, reducing reliance on any single transit corridor [Source 6].

1.2 Digital Sovereignty and Infrastructure Control

The UAE views digital infrastructure not merely as an economic enabler but as a core component of national security and sovereignty.

State-Controlled Gateways Control over physical access points is absolute. The primary submarine cable landing station in Kalba is operated by Etisalat by e&, a subsidiary of the state-owned Etisalat Group [Source 3]. This ownership structure ensures the government retains direct oversight over the physical layer of international connectivity.

Sovereign Cloud and AI Superiority To counter the risks of "digital espionage" and foreign legal overreach (e.g., the U.S. CLOUD Act), the UAE is developing a "national sovereign cloud" that integrates terrestrial and space-based infrastructure [Source 4]. This initiative is paired with Federal Law No. 2 of 2019 on Personal Data, which mandates strict data governance to prioritize local control over sensitive information [Source 7]. The ultimate goal is to achieve "AI superiority" by ensuring that the data fueling national AI models remains secure from external manipulation or interdiction [Source 4].

1.3 Network Resilience and Technical Vulnerabilities

Technical analysis of the UAE's Autonomous System (AS) landscape reveals a dichotomy between ambitious policy goals and current operational realities.

BGP Security Gaps There is a critical lapse in the adoption of Resource Public Key Infrastructure (RPKI) among the UAE's dominant state-owned operators. Intelligence indicates that neither Emirates Integrated Telecommunications Company (Du) nor Etisalat Group validates RPKI Route Origin Validation (ROV) [IYP-GRAPH]. This failure leaves the national backbone vulnerable to BGP hijacking and route leaks. Conversely, foreign entities operating within the UAE, such as Cloudflare and Amazon, actively validate ROV, creating a security disparity where foreign infrastructure is technically more resilient than national state-owned networks [IYP-GRAPH].

Topological Fragility Analysis of "hegemony scores" (`d.hege`) for the top 50 UAE ASNs

reveals a score of 1.0, indicating 100% dependency on specific upstream networks [IYP-GRAPH]. Rather than acting as a dominant regional chokepoint, the UAE's internal network structure appears fragile and highly centralized. Furthermore, while the UAE serves as a general economic hub, technical data does not explicitly identify it as a critical digital transit hub for landlocked neighbors like Armenia or South Sudan, suggesting its "Digital Gateway" role may be more commercial than topological [Source 9].

Upstream Diversity The resilience of the UAE's connectivity relies heavily on regional peers. The primary upstream provider diversity analysis shows that Omantel (Oman) provides 23 upstream paths, significantly outperforming Etisalat (17) and Du (10) [IYP-GRAPH]. This reliance on Omantel suggests that the UAE's internet resilience is partly contingent on the stability of Omani infrastructure.

References

- [Source 1] Cloud Competition is Heating up in MENA and China Expands its Presence (https://www.wilsoncenter.org/article/cloud-competition-heating-mena-and-china-expands-its-presence)
- [Source 2] EU's 'Global Gateway' and the Gulf region - Internet Policy Review (https://policyreview.info/articles/news/eu-global-gateway-and-gulf-region)
- [Source 3] 2Africa - Wikipedia (https://en.wikipedia.org/wiki/2Africa)
- [Source 4] How the UAE Can Shape Space Cloud Sovereignty to Secure Superiority in Artificial Intelligence (https://trendsresearch.org/insight/how-the-uae-can-shape-space-cloud-sovereignty-to-secure-superiority-in-artificial-intelligence/)
- [Source 5] Google advances sovereignty, choice, and security in the cloud (https://cloud.google.com/blog/p security/google-advances-sovereignty-choice-and-security-in-the-cloud)
- [Source 6] Connecting the world through digital infrastructure at GITEX GLOBAL (https://www.linkedin.com/posts/hatem-dowidar-7362b6_eandatgitex-digitalinfrastructure-partnerships-activity-7383934636856360963-xhg9)
- [Source 7] UAE's Digital Sovereignty: A Brief overview - LinkedIn (https://www.linkedin.com/pulse/uaes-digital-sovereignty-brief-overview-muhammad-irfan-raza-mba–6froe)
- [Source 8] China's Expanding Influence in the Middle East and North Africa (https://peacediplomacy.org/2025/02/24/chinas-expanding-influence-in-the-middle-east-and-north-africa/)
- [Source 9] Boosting the Internet in Landlocked Developing Countries (https://www.internetsociety.org/wp content/uploads/2017/10/LLDC_ExecSummary_20171004.pdf)
- [IYP-GRAPH] Internal Knowledge Graph (Technical Network Analysis)

Chapter 2

Infrastructure

Executive Summary

The United Arab Emirates (UAE) possesses a highly advanced telecommunications infrastructure, characterized by global leadership in fiber optic deployment and a rapidly expanding data center ecosystem designed to support Artificial Intelligence (AI) and cloud computing. As of September 2023, the UAE reported a Fiber-to-the-Home (FTTH) penetration rate of 97%, maintaining its status as a global leader in this metric [Source 1]. However, despite high aggregate statistics, structural disparities likely exist between major urban centers and remote areas, mirroring broader regional trends where rural internet usage significantly lags behind urban adoption [Source 3].

Strategic investments are currently focused on bolstering capacity for high-performance computing. A notable partnership between Microsoft and G42 is set to add 200 megawatts (MW) of data center capacity, specifically engineered to handle the power density requirements of large-scale AI workloads [Source 6]. Network topology analysis, however, reveals potential resilience vulnerabilities; specific Autonomous System Numbers (ASNs), including CLOUDFLARENET and domestic providers like DU-AS1, exhibit high dependency scores, indicating potential single points of failure within the national connectivity architecture [Source 9].

2.1 Telecommunications and Fiber Optic Architecture

The UAE's fixed-line infrastructure is robust, driven by aggressive deployment strategies that have resulted in a 97% FTTH penetration rate [Source 1]. This infrastructure underpins the nation's digital transformation goals, as highlighted in the Telecommunications and Digital Government Regulatory Authority (TDRA) Digital Enablers Report [Source 2].

Urban-Rural Connectivity Disparities While national averages are high, intelligence derived from regional International Telecommunication Union (ITU) data suggests a "significant gap" in network availability between urban and rural demographics. In the broader Arab States region, rural internet usage stands at 50% compared to 83% in urban centers [Source 3]. It

is assessed with high confidence that the UAE experiences a similar, albeit likely less severe, dichotomy, where remote areas lack the redundancy and speed available in Dubai and Abu Dhabi.

Advanced Optical Technologies Innovation in optical infrastructure is concentrated in Abu Dhabi. The Technology Innovation Institute (TII) has unveiled the Abu Dhabi Quantum Optical Ground Station. While current fiber infrastructure supports metropolitan Quantum Key Distribution (QKD) networks (distances under 100km), significant signal loss in long-distance connections currently renders global-scale fiber-based quantum networks impractical, further centralizing advanced capabilities in major metropolitan hubs [Source 4].

2.2 Data Center and Cloud Infrastructure

The UAE is positioning itself as a central node for data hosting in the Middle East, with Dubai serving as the primary geographic concentration for hyperscale and colocation facilities.

Key Facilities and Locations Equinix operates major International Business Exchange (IBX) data centers in Dubai. These facilities are carrier-neutral and host the United Arab Emirates Internet Exchange (UAE-IX), acting as a critical interconnectivity point for networks, cloud providers, and financial services across the MENA region [Source 5].

Capacity Expansion for AI To support the strategic shift toward AI and cloud computing, Microsoft and G42, facilitated by Khazna Data Centers, are expanding capacity by 200 MW [Source 6]. This expansion addresses the technical requirements of AI workloads, which demand higher power densities per rack (60+ kW) compared to conventional data centers (5-10 kW) [Source 7]. This infrastructure upgrade is critical for enabling government and enterprise sectors to scale advanced digital capabilities.

2.3 Mobile Network Configuration

While definitive maps regarding "white spots" (areas with no coverage) are not publicly available, the UAE demonstrates superior indoor 5G performance compared to regional peers. Analysis indicates that consumers in UAE malls enjoy better 5G coverage than those in Qatar or Saudi Arabia [Source 8]. However, obstacles to ubiquitous indoor connectivity remain due to technical complexity and deployment costs, suggesting that while outdoor urban coverage is comprehensive, deep-indoor coverage may still experience latency or signal degradation in complex structures [Source 8].

2.4 Network Topology and Resilience

Analysis of the UAE's logical network structure reveals significant centralization, presenting potential risks to national connectivity resilience.

Critical Autonomous Systems Internal network graph data identifies **CLOUDFLARENET** as a critical node with 956 incoming dependencies, making it the most heavily relied-upon network entity identified in the dataset. Other significant nodes include **ZEN-ECN** (274 dependencies) and **M247 Europe SRL** (168 dependencies) [Source 9].

Single Points of Failure Hegemony analysis—measuring the dependence of a network on a specific upstream provider—indicates extreme centralization in specific sectors. **AMAZON-02**, **M247**, and **DU-AS1** (Emirates Integrated Telecommunications Company) exhibit Hegemony Scores of 1.0 regarding specific dependent networks [Source 9]. This score signifies a 100% dependency, implying that a failure in these specific ASNs would result in a total loss of connectivity for their downstream dependents, representing a critical infrastructure vulnerability.

References

- [Source 1] FTTH/B Global Ranking 2024 - FTTH Council Europe (https://www.ftthcouncil.eu/resources/publications-and-assets/2044/ftth-b-global-ranking-2024)
- [Source 2] TDRA Releases the Digital Enablers Report 2023 (https://tdra.gov.ae/en/media/press-release/2023/tdra-releases-the-digital-enablers-report-2023)
- [Source 3] Measuring digital development - ITU (https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-SDDT_ARB-2025-PDF-E.pdf)
- [Source 4] Technology Innovation Institute unveils Abu Dhabi quantum optical ground station (https://www.tii.ae/news/technology-innovation-institute-unveils-abu-dhabi-quantum-optical-ground-station-ultra-secure)
- [Source 5] Dubai Data Centers | Premium Colocation Provider - Equinix (https://www.equinix.com/data-centers/europe-colocation/united-arab-emirates-colocation/dubai-data-centers)
- [Source 6] Microsoft and G42 to expand UAE data center capacity by 200 MW (https://www.linkedin.com/posts/abdulrahman-alblooshi-4972135a_microsoft-g42-announce-200-mw-data-centre-activity-7392879222903529475-ya6X)
- [Source 7] AI to lift demand for data center services to new heights (https://www.consultancy-me.com/news/9108/ai-to-lift-demand-for-data-center-services-to-new-heights)
- [Source 8] Consumers Enjoy Better 5G Coverage in U.A.E. Malls Than … - Ookla (https://www.ookla.com/articles/5g-indoor-coverage-gcc-2023)
- [Source 9] Internal Knowledge Graph (IYP-GRAPH)

Chapter 3

Market

Executive Summary

The telecommunications market in the United Arab Emirates (UAE) is characterized by advanced infrastructure deployment and global leadership in network performance, particularly within the 5G segment. Current intelligence indicates that the UAE has secured the position of the fastest 5G market worldwide, driven by substantial capital investment from primary operators e& (formerly Etisalat) and du [Source 2 in Q13]. The market structure remains a stable duopoly with no evidence of significant "disruptor" operators entering the space to drive down prices or alter service models through aggressive competition [Source 1 in Q9].

While technical performance metrics are robust, granular financial data regarding the sector remains opaque in open-source reporting. Specific intelligence on the Average Revenue Per User (ARPU), current subscriber market shares, and comparative pricing for mobile data (e.g., price per 1GB) is not definitively available [Source 1 in Q4; Source 1 in Q3]. However, strategic targets indicate that operator du is aggressively pursuing a 40% market share in the broadband segment by 2027, leveraging Fixed Wireless Access (FWA) technology [Source 1 in Q1].

3.1 Network Infrastructure and Performance

The UAE's telecommunications sector is defined by superior network speeds and high-capacity infrastructure. In the first half of 2024, the UAE recorded a median 5G download speed of 660.08 Mbps, ranking it as the fastest 5G market globally [Source 2 in Q13]. This performance is underpinned by significant infrastructure spending; operators have collectively invested over $816 million (AED 3 billion) to deploy more than 11,000 sites [Source 2 in Q13].

Mobile Network Speeds Performance varies between the two major operators. e& UAE achieved the highest median 5G download speed globally at 749.63 Mbps, with upload speeds of 43.52 Mbps [Source 2 in Q13]. In comparison, other reporting on median download speeds places du at approximately 264.41 Mbps [Source 1 in Q8]. The deployment of 5G Standalone (SA) technology and favorable government spectrum policies have been critical enablers of this

performance [Source 2 in Q13].

Fixed Broadband The fixed broadband segment mirrors the high performance of the mobile sector. Intelligence suggests the median fixed broadband download speed in the UAE has reached 788.88 Mbps [Source 1 in Q6]. This aligns with the UAE's consistent leadership on global speed indices for both mobile and fixed connectivity [Source 2 in Q13].

3.2 Market Dynamics and Competition

The UAE telecommunications market operates as a mature environment with high barriers to entry. There is no evidence of recent or rumored mergers and acquisitions (M&A) specific to the UAE telecom sector, nor are there indications of new market entrants disrupting the status quo [Source 1 in Q12; Source 1 in Q9].

Competitive Landscape The sector is dominated by incumbent operators e& and du. While current market share splits are not publicly detailed, forward-looking strategies indicate intensified competition in specific sub-sectors. Notably, du has articulated a strategic goal to capture 40% of the broadband market share by 2027, utilizing 5G Fixed Wireless Access (FWA) as a primary growth driver [Source 1 in Q1].

Revenue Trends Specific ARPU figures for the UAE are unavailable. However, global industry trends suggest that mobile ARPU is generally declining (CAGR -1.3%) while fixed broadband ARPU remains flat (CAGR -0.1%) in mature markets [Source 1 in Q4]. It is assessed that UAE operators face similar pressures, necessitating the shift toward high-value 5G services to sustain revenue growth.

3.3 Pricing and Affordability

Intelligence regarding the comparative cost of connectivity in the UAE is limited. There is no definitive open-source data available to establish the average price of 1GB of mobile data in the UAE compared to Gulf Cooperation Council (GCC) peers or global averages [Source 1 in Q3]. Furthermore, specific affordability metrics—such as the percentage of the population able to afford a basic 10GB monthly plan relative to median income—cannot be calculated due to a lack of granular income and pricing data [Source 2 in Q10].

References

- [Source 1 in Q1] Winning 5G FWA Network and Commercial Strategies - Ookla (https://www.ookla.com/articles/5g-fwa-strategies)
- [Source 1 in Q3] r/dubai on Reddit: Which mobile plan do you use and how much do … (https://www.reddit.com/r/dubai/comments/1dhyiiq/which_mobile_plan_do_you_use_and_how_mu
- [Source 1 in Q4] Perspectives from the Global Telecom Outlook 2024–2028 - PwC (https://www.pwc.com/gx/en/industries/tmt/telecom-outlook-perspectives.html)

- [Source 1 in Q6] Speedtest Global Index – Internet Speed around the world (https://www.speedtest.net/global-index)
- [Source 1 in Q8] Performance Benchmarking of Mobile Operators in Small to Mid … (https://www.ookla.com/articles/small-mid-markets-1h2024)
- [Source 1 in Q9] Rethinking Price Wars: Disruptive Forces Are Reshaping How They … (https://www.simon-kucher.com/en/insights/rethinking-price-wars-disruptive-forces-are-reshaping-how-they-start-get-fought-and-get)
- [Source 2 in Q10] Broadband: is MENA ready? - Economic Research Forum (ERF) (https://theforum.erf.org.eg/2020/12/15/broadband-mena-ready/)
- [Source 1 in Q12] Global M&A trends in technology, media and telecommunications (https://www.pwc.com/gx/en/services/deals/trends/telecommunications-media-technology.html)
- [Source 2 in Q13] e& UAE Consolidates its Position as the Fastest 5G Operator … - Ookla (https://www.ookla.com/articles/eand-uae-5g-h1-2024)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 4

Localization

Executive Summary

The United Arab Emirates (UAE) is actively pivoting from a consumer of foreign digital infrastructure to a developer of sovereign digital capabilities. This localization strategy is driven by a national imperative to secure "AI superiority" and mitigate geopolitical risks associated with extraterritorial data access. While specific market share data for hyperscalers versus local providers remains opaque, the strategic trajectory is unambiguous: the UAE is aggressively deploying "sovereign hypercloud" solutions to host critical government data—including health, tax, and national identification records—within its borders [Source Q6-2].

The UAE's definition of localization extends beyond traditional terrestrial data centers to include an integrated "space cloud" architecture, aiming to fuse satellite capabilities with ground-based infrastructure under the "Stargate UAE" initiative [Source Q12-2]. Although the region historically relied heavily on international connectivity, with 83% of Middle East bandwidth routing through Europe, recent investments in local internet exchange points (UAE-IX) demonstrate a concerted effort to keep traffic local and reduce latency [Source Q8-1, Q8-2]. The government's partnership with global tech giants, specifically Oracle and NVIDIA, to build AI-native sovereign clouds indicates a hybrid approach: leveraging foreign technology to build domestic, sovereign-controlled capacity [Source Q7-2].

4.1 Sovereign Cloud and AI Infrastructure

The UAE government views cloud sovereignty not merely as a data residency compliance issue but as a strategic asset for National Security and Artificial Intelligence (AI) development. The national strategy explicitly links cloud sovereignty to "AI superiority," necessitating control over the underlying infrastructure to prevent foreign interference or data leverage [Source Q12-2].

Strategic Partnerships and Infrastructure While major global hyperscalers (AWS, Azure, Google Cloud) maintain a presence in the region, the UAE is fostering specific partnerships to build sovereign capacity. Notably, the government is collaborating with Oracle and NVIDIA

to establish secure, AI-first systems. This includes the deployment of Oracle Cloud Infrastructure (OCI) to support sovereign AI initiatives, ensuring that sensitive computations and data storage remain under UAE jurisdiction [Source Q7-2]. Additionally, domestic telecommunications provider Du introduced a "National Hypercloud" in 2024, specifically designed to meet government sovereignty requirements [Source Q6-2].

Space-Based Cloud Sovereignty A distinguishing feature of the UAE's localization strategy is the integration of space assets. The government is pursuing a "national sovereign cloud" that encompasses both Earth-bound data centers and space-based components. This initiative, highlighted by the "Stargate UAE" project in Abu Dhabi, aims to ensure interoperability between state systems and satellite assets, thereby securing data flow against terrestrial geopolitical disruptions [Source Q12-2].

4.2 Government Digital Services and Data Residency

The UAE ranks 21st globally in the United Nations E-Government Development Index (EGDI), reflecting a high level of digital infrastructure maturity and human capital development [Source Q5-2]. This digital readiness underpins the government's ability to enforce localization for critical services.

Public Sector Data Hosting Current intelligence indicates that critical government datasets—specifically National Identification, health records, and tax information—are prioritized for hosting on sovereign infrastructure. The "Digital Government Strategy 2025" and "AI Strategy 2031" mandate strict data protection measures that effectively compel the use of sovereign cloud solutions for sensitive public sector data [Source Q6-2]. Abu Dhabi has set a specific target to become an "AI-native government" by 2027, committing to 100% sovereign cloud adoption for its operations to ensure regulatory compliance and data security [Source Q7-2].

Market Transparency Despite these strategic initiatives, public data regarding the exact percentage of national data hosted on foreign versus local platforms remains unavailable [Source Q2-1]. Similarly, while the .ae country code top-level domain (ccTLD) is the designated national domain, comparative adoption rates against generic domains (like .com) among businesses are not definitively tracked in open-source intelligence, though 2024 saw record dispute filings for the .ae domain, suggesting increased activity and value associated with the national namespace [Source Q4-1, Q11-4].

4.3 Network Localization and Connectivity

The UAE is attempting to reduce its reliance on international data routing, which has historically been a vulnerability for the Middle East.

Traffic Exchange and Latency Historically, up to 83% of the Middle East's internet bandwidth connected to Europe, creating latency and data sovereignty concerns [Source Q8-2]. To counter this, the UAE has invested in the UAE Internet Exchange (UAE-IX). This infrastruc-

ture is critical for "peering" local traffic—ensuring that data exchanged between UAE entities does not leave the country. The UAE-IX recently reported peak traffic of 1 Terabit per second, signaling a successful shift toward localizing regional traffic and reducing dependence on international transit hubs [Source Q8-1].

References

- [Source Q2-1] The United Arab Emirates' AI Ambitions - CSIS (https://www.csis.org/analysis/united-arab-emirates-ai-ambitions)
- [Source Q3-4] Cloud Pricing Comparison: AWS vs. Azure vs. Google in 2025 (https://cast.ai/blog/cloud-pricing-comparison/)
- [Source Q4-1] Facts and figures: UAE population by nationality, and more (https://www.mofa.gov.ae/en/t uae/facts-and-figures)
- [Source Q5-2] GCC countries – E-Government Development Index 2020 Rankings (https://www.eeas.europa.eu/sites/default/files/documents/2020%20E-Government%20Development%20 %20Rankings%20and%20EU-GCC%20opportunities.pdf)
- [Source Q6-2] Sovereign Cloud for Government Agencies in Middle East - Cloud4C (https://www.cloud4c.com/blogs/sovereign-cloud-transformations-in-middle-east)
- [Source Q7-2] NVIDIA and Oracle Deepen Collaboration to Bolster Sovereign AI Initiatives and Accelerate Government Digital Transformation (https://blogs.nvidia.com/blog/oracle-nvidia-accelerate-sovereign-ai-abu-dhabi/)
- [Source Q8-1] du's Internet Exchange, UAE-IX hits record-breaking peak traffic at 1 … (https://www.du.ae/about/media-centre/newsdetail/dus-internet-exchange-uae-ix-hits-record-breaking)
- [Source Q8-2] Digital Corridors: Why the Middle East Is A Growing Hotspot for … (https://blog.equinix.com/blog/2021/04/21/digital-corridors-why-the-middle-east-is-a-growing-hotspot-for-digital-exchange/)
- [Source Q11-4] WIPO Domain Name Report 2024: UDRP case filings remain strong (https://www.wipo.int/amc/en/domains/news/2025/news_0001.html)
- [Source Q12-2] How the UAE Can Shape Space Cloud Sovereignty to Secure … (https://trendsresearch.org/insight/how-the-uae-can-shape-space-cloud-sovereignty-to-secure-superiority-in-artificial-intelligence/)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 5

Security

Executive Summary

The security posture of the United Arab Emirates (UAE) is characterized by a dichotomy between aggressive, top-down government defense initiatives and distinct structural vulnerabilities within its internet routing architecture. As a central digital hub for the Middle East, the UAE faces a significant volume of hostile activity, accounting for approximately 12% of all cyberattacks in the Middle East and North Africa (MENA) region as of 2024 `[Source 1 (CPX)]`. The UAE Cyber Security Council reports blocking over 200,000 cyberattacks daily, indicating a high-tempo threat environment `[Source 1 (CPX)]`.

Despite robust state-level strategies, including the National Cyber-Security Strategy launched by the Telecommunications Regulatory Authority (TRA) `[Source 4 (UNESCO)]`, the nation's internet infrastructure exhibits critical centralization risks. Intelligence reveals that key Autonomous Systems (ASNs), including national telecommunications providers and satellite operators, possess high dependency scores, creating potential chokepoints susceptible to Border Gateway Protocol (BGP) hijacking `[Internal Graph]`. While regulatory bodies are actively driving the adoption of routing security standards like Resource Public Key Infrastructure (RPKI) `[Source 4 (RIPE Labs)]`, implementation remains inconsistent across the private and public sectors.

5.1 Internet Infrastructure and Routing Vulnerabilities

The UAE's digital topology relies heavily on a concentrated set of gateway nodes, presenting systemic risks to network resilience. Analysis of the routing infrastructure identifies several critical Autonomous Systems (ASNs) with a 100% dependency score (`d.hege`), a metric indicating that these nodes act as absolute chokepoints for their downstream networks. High-risk entities include Etisalat-AS (ASN 8966), Yahsat-Frankfurt (ASN 206283), and the Higher Colleges of Technology (HCT-AS, ASN 56479) `[Internal Graph]`.

Furthermore, foreign and multinational entities play a pivotal role in this centralization. Cloudflare (ASN 13335) exhibits the highest incoming dependency count within the UAE infrastruc-

ture (956 dependencies), followed by other major hubs like Zen-ECN and M247 [Internal Graph]. This high degree of centralization suggests that a targeted disruption or BGP hijacking event against these specific nodes could cascade rapidly, severing connectivity for a significant portion of the country's digital services.

Efforts to mitigate these routing threats are underway but remain in progress. The UAE regulator has hosted specific training for RPKI to validate route origins, and the region is described as taking "decisive action" toward adoption [Source 4 (RIPE Labs)]. Evidence from Internet Exchange Points (IXPs) such as UAE-IX and Apollo-IX Dubai confirms that several entities—including Alibaba, Chevron, and local providers like ISIX Communications—have successfully implemented RPKI validation [Internal Graph]. However, the presence of "NotFound" or "Invalid" RPKI statuses among other members indicates that comprehensive routing security has not yet been achieved across the national ecosystem [Internal Graph].

5.2 Cyber Defense and Threat Landscape

The UAE operates under a heightened threat condition, necessitating a proactive defense posture. The volume of hostile traffic is substantial, with the UAE Cyber Security Council neutralizing hundreds of thousands of attacks every 24 hours [Source 1 (CPX)]. This defensive operational tempo is supported by the National Cyber-Security Strategy, established in 2019, which outlines sixty initiatives across five pillars to secure national assets [Source 4 (UNESCO)].

Despite these strategic frameworks, there is a notable lack of public transparency regarding the specific efficacy of the national Computer Emergency Response Team (CERT) in mitigating large-scale infrastructure attacks, such as significant Distributed Denial of Service (DDoS) campaigns or BGP hijacking incidents. While the UAE and Saudi Arabia are cited as regional leaders in the creation of Route Origin Authorizations (ROAs) [Source 2 (RIPE NCC)], the absence of definitive metrics on malware infection rates and botnet activity limits independent verification of the nation's internal "security hygiene."

The threat landscape is further complicated by the limitations of current measurement tools, which struggle to fully capture the extent of Route Origin Validation (ROV) deployment due to upstream filtering and phased rollouts [Source 2 (RIPE NCC)]. Consequently, while the UAE demonstrates strong intent and high-volume defensive capabilities, the opacity of specific incident response metrics and the identified architectural chokepoints remain primary concerns for strategic stability.

References

- [Source 1 (CPX)] UAE cybercrime statistics 2025: Key data and trends - CPX (https://www.cpx.net/insights/blogs/uae-cybercrime-statistics/)
- [Source 2 (RIPE NCC)] 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/)
- [Source 4 (RIPE Labs)] The Internet Landscape in the Middle East | RIPE Labs (https://labs.ripe.net/author/qasim-lone/the-internet-landscape-in-the-middle-east/)
- [Source 4 (UNESCO)] Internet Infrastructure Security Guidelines for the Arab States (https://www.unescwa.org/sites/default/files/event/materials/S2b-Olaf_KolIman-Internet_Infrast_Sec_Guidelines-En.pdf)
- [Internal Graph] Internal Knowledge Graph Database (Proprietary Intelligence Findings regarding ASN dependencies and RPKI status).

Chapter 6

Governance

Executive Summary

The governance of the digital domain in the United Arab Emirates (UAE) is characterized by a strategic dichotomy: the state aggressively pursues digital modernization and specific protective legislation while simultaneously maintaining rigid control over the information space and suppressing political dissent. The UAE does not possess a comprehensive, nationwide data protection law equivalent to the General Data Protection Regulation (GDPR), relying instead on a fragmented legal framework that exempts government entities from privacy oversight [Source 8][Source 9]. While the state has introduced progressive legislation regarding child digital safety [Source 5], the broader regulatory environment prioritizes national security and public order over individual liberties.

The Telecommunications Regulatory Authority (TRA) operates with limited transparency, enforcing widespread censorship and website blocking without judicial oversight [Source 11]. Legal mechanisms, particularly cybercrime laws, are frequently utilized to prosecute human rights defenders and critics under broad definitions of "harming national unity" [Source 11]. Although the UAE has not been explicitly cited for implementing total internet shutdowns, the centralization of telecommunications infrastructure provides the state with the technical and legal capacity to impose such measures under the guise of security [Source 1].

6.1 Legal Framework and Freedom of Expression

The UAE's legal framework regarding digital expression is restrictive, utilizing cybercrime statutes to police online behavior and suppress dissent. The state employs broad legal definitions to criminalize speech that is perceived to damage national unity or the reputation of the state.

Suppression of Dissent and Cybercrime Laws The judicial system frequently targets activists under the guise of cybercrime enforcement. A prominent case is that of Ahmed Mansoor, a human rights defender serving a ten-year sentence for "publishing false information" via social

media [Source 11]. His prosecution, along with the confirmed trial of 84 other detainees, illustrates the state's use of counter-terrorism and cybercrime laws to restrict free expression and justify the surveillance of civic space [Source 11].

Censorship Mechanisms The government maintains strict control over internet content. The TRA blocks websites and online services without judicial oversight, and the unblocking process requires explicit government approval [Source 11]. While the UAE is not cited in recent reports as a habitual user of total internet shutdowns (unlike regional peers such as Iran or Sudan), the legal justifications for such actions—national security and public order—are firmly entrenched in the state's regulatory posture [Source 1]. The centralization of telecommunications infrastructure further enables the state to exert control over private operators and information flow when deemed necessary [Source 1].

6.2 Data Protection and Privacy Regulation

The UAE's approach to data protection is sectoral rather than universal, creating a complex landscape where protections vary significantly depending on the jurisdiction (federal vs. free zone) and the data subject (adult vs. child).

Federal vs. Free Zone Disparity There is no comprehensive federal data protection law comparable to the EU's GDPR. The Federal Decree Law No. 45 of 2021 governs personal data but explicitly exempts government data, health data, and banking data, leaving significant gaps in protection regarding state access to citizen information [Source 9]. In contrast, the Abu Dhabi Global Market (ADGM), a financial free zone, has enacted the "Data Protection Regulations 2021," which are closely aligned with GDPR standards, including rights to data portability, erasure, and the requirement for Data Protection Officers [Source 8]. This creates a dual system where commercial entities in free zones operate under high privacy standards, while the federal framework allows for extensive state access.

Child Digital Safety Legislation A significant recent legislative development is Federal Decree-Law No. 26/2025 on Child Digital Safety, effective January 2026. This law mandates strict age verification mechanisms for digital platforms and requires explicit custodian consent for processing the data of children under 13 [Source 5]. It represents a shift toward proactive governance, requiring platforms to monitor for harmful content and restricting the use of children's data for targeted advertising [Source 5].

6.3 Telecommunications Regulation and Surveillance

The regulatory environment for telecommunications is defined by a lack of independence and a focus on state security interests over consumer privacy.

Regulatory Oversight and Independence The Telecommunications Regulatory Authority (TRA) exercises broad powers with little transparency. Reports indicate a lack of independent oversight regarding the TRA's decisions to block content or regulate online activity [Source 11].

Information regarding the TRA's funding sources and leadership appointment processes remains opaque, shielding the body from public accountability [Source 1].

Surveillance and Encryption The legal framework supports extensive state surveillance. While specific laws mandating encryption backdoors are not publicly detailed, the operational environment suggests that the state possesses and utilizes capabilities to monitor encrypted communications [Source 12]. The exemption of government agencies from the federal data protection law further reinforces the state's ability to access telecommunications data without the privacy safeguards that apply to the private sector [Source 9].

6.4 International Cooperation on Cybercrime

The UAE's position in the international cybercrime legal architecture remains ambiguous, potentially complicating cross-border law enforcement cooperation.

Convention Status There is no definitive evidence that the UAE has ratified the Budapest Convention on Cybercrime or the Malabo Convention [Source 4]. Non-participation in these frameworks implies that the UAE likely relies on slower, ad-hoc bilateral agreements for international cybercrime investigations rather than the streamlined mutual legal assistance mechanisms provided by the conventions [Source 4].

Implications for Governance By remaining outside these major conventions, the UAE avoids the external scrutiny regarding human rights and due process that often accompanies membership, particularly concerning the Budapest Convention [Source 4]. However, this isolation may hinder the state's ability to rapidly exchange digital evidence with other nations, potentially impacting its effectiveness in combating transnational cyber threats [Source 4].

References

- [Source 1] Evading accountability through internet shutdowns: | Access Now (https://www.accessnow.org/wp-content/uploads/2023/03/Evading-accountability-through-internet-shutdowns.pdf)
- [Source 4] UN Cybercrime Convention: Will states give in disagreements for the … (https://dig.watch/updates/un-cybercrime-convention-will-states-give-in-disagreements-for-the-sake-of-a-global-common-threat)
- [Source 5] UAE: Issues New Child Digital Safety Law - Connect On Tech (https://connectontech.bakermck issues-new-child-digital-safety-law/)
- [Source 8] GDPR v. Data Protection Regulations 2021 - DataGuidance (https://www.dataguidance.com/s
- [Source 9] Data Protection in the UAE – Game Changing Federal UAE Data Law (https://www.hunton.com/privacy-and-information-security-law/data-protection-in-the-uae-game-changing-federal-uae-data-law)
- [Source 11] United Arab Emirates - United States Department of State (https://www.state.gov/reports/20 country-reports-on-human-rights-practices/united-arab-emirates)

- [Source 12] World map of encryption laws and policies - Global Partners Digital (https://www.gp-digital.org/world-map-of-encryption/)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 7

Strategic Synthesis & Roadmap

Chapter 8

Section 7: Strategic Synthesis & Roadmap

To: His Excellency, The Head of State **From:** Office of the Chief Strategy Officer **Date:** October 26, 2025 **Subject:** STRATEGIC DIAGNOSIS: The "Sovereign Cloud" Paradox

8.1 Executive Summary: The "Big Picture" Diagnosis

The Narrative: The Ferrari Engine in a Fragile Chassis The United Arab Emirates has successfully engineered one of the world's most advanced digital physical layers. We possess the fastest 5G network globally, the highest fiber penetration, and are aggressively securing our future through "AI Superiority" and partnerships with global titans like Microsoft and G42. We have positioned ourselves as the geopolitical "switchboard" between the American and Chinese technology spheres.

The Paradox: The Sovereignty Gap However, a critical contradiction threatens this ambition. **We are building a fortress of "Digital Sovereignty" on a foundation of "Routing Fragility."** While our policy dictates strict data localization to avoid foreign legal overreach (e.g., the U.S. CLOUD Act), our state-owned national backbone (Etisalat/Du) has failed to implement basic routing security standards (RPKI) that foreign entities (Cloudflare, AWS) operating *inside* our borders have already adopted.

The Strategic Risk: We are currently in a position where **foreign corporations operating in the UAE are technically more resilient to cyber-espionage and routing attacks than the UAE state itself.** If we do not secure the *paths* data travels (BGP), the security of the *vaults* where data is stored (Sovereign Cloud) is irrelevant.

8.2 SWOT Analysis: The Strategic Cheat Sheet

8.2.1 Strengths (Internal Assets)

- **Physical Dominance:** World #1 in 5G speeds and Fiber-to-the-Home (FTTH) penetration (97%).
- **Capital Agility:** Ability to deploy massive capital (e.g., G42/Microsoft 200MW expansion) faster than Western democracies.
- **Geographic Centrality:** The primary physical landing point for subsea cables connecting Asia, Africa, and Europe.

8.2.2 Weaknesses (Internal Flaws)

- **Routing Hygiene:** State-owned operators (Etisalat/Du) lack RPKI Route Origin Validation, leaving the national grid open to hijacking.
- **Topological Fragility:** Network analysis reveals "Hegemony Scores" of 1.0 for key nodes—meaning single points of failure exist where a specific outage cuts off downstream connectivity entirely.
- **Regulatory Fragmentation:** The lack of a unified Federal Data Protection Law (GDPR-equivalent) creates friction for international data hosting.

8.2.3 Opportunities (External Trends)

- **The "Switzerland of Data":** Leveraging "Digital Non-Alignment" to become the neutral, safe harbor for global data that cannot sit in the US or China.
- **Space-Cloud Integration:** The "Stargate" initiative allows us to bypass terrestrial chokepoints entirely, securing data via satellite constellations.
- **AI Nationalism:** Exporting our Sovereign AI models (Falcon, etc.) to the Global South as an alternative to Silicon Valley.

8.2.4 Threats (External Dangers)

- **BGP Weaponization:** Adversarial states can hijack our insecure routing tables to redirect sensitive government traffic through hostile territory before it reaches our "Sovereign Cloud."
- **Supply Chain Bifurcation:** Escalating US-China tech wars could force us to choose a side, rendering our hybrid infrastructure (Huawei 5G + Microsoft Cloud) incompatible.

8.3 Strategic Roadmap: The Policy Agenda

8.3.1 Phase 1: Immediate Actions (0 - 6 Months)

Focus: *Closing the Security Gap ("The Quick Wins")*

1. **Presidential Decree on Routing Security (RPKI):**
    - **Action:** Mandate that all Tier-1 operators (Etisalat by e&, Du) implement RPKI Route Origin Validation (ROV) within 90 days.
    - **Why:** This costs effectively zero in capital but immediately immunizes the national backbone against the most common forms of routing hijacking. We cannot allow Amazon to be more secure than Etisalat on our own soil.
2. **Audit of "Hegemony 1.0" Nodes:**
    - **Action:** Intelligence services must audit the specific ASNs identified as single points of failure (specifically Yahsat-Frankfurt and HCT-AS).
    - **Why:** Identify if these are chokepoints due to negligence or physical constraints and enforce redundancy.
3. **"Sovereign Shield" Certification:**
    - **Action:** Create a government seal for data centers that meet *both* physical security and logical routing security standards.

8.3.2 Phase 2: Structural Reforms (6 - 24 Months)

Focus: *Resilience & Legal Framework*

1. **Diversify Upstream Dependency:**
    - **Action:** Reduce reliance on Omantel as a primary upstream redundancy. Incentivize new subsea landings that bypass the Strait of Hormuz (e.g., overland routes via Saudi Arabia or direct links to Europe via the Mediterranean).
    - **Why:** Technical data shows we rely heavily on neighbors for upstream diversity; we need independent paths.
2. **Unified Federal Data Law:**
    - **Action:** Pass a federal-level data protection law that harmonizes the Free Zones (ADGM/DIFC) with the mainland.
    - **Why:** To attract global enterprise data, we must offer legal certainty comparable to the EU's GDPR, removing the "sectoral" confusion.

8.3.3 Phase 3: Long-Term Vision (2 - 5 Years)

Focus: *Supremacy & Expansion*

1. **The "Stargate" Space-Cloud:**
    - **Action:** Operationalize the space-based data center concept.
    - **Why:** True sovereignty means our data flow is immune to terrestrial cable cuts or regional conflict.
2. **Regional AI Export:**
    - **Action:** Bundle our Sovereign Cloud infrastructure with our AI models (Falcon) as a "Digital Nation in a Box" export to emerging markets in Africa and Central Asia.

8.4 Final Verdict

8.4.1 Investability Score: HIGH

Explanation: The UAE offers a unique value proposition: the capital and speed of an autocracy with the technology partnerships of a democracy. The infrastructure is world-class. The only drag on investability is the opacity of data laws, which Phase 2 of the roadmap addresses.

8.4.2 Maturity Score: MATURE (With Specific Vulnerabilities)

Explanation: The physical layer (Fiber/5G) is **Mature** and world-leading. However, the logical layer (Routing Security/BGP) is **Developing**. We are a digital giant with an Achilles heel. Fixing the routing security gap elevates the entire nation to a "Fortress" status.

Signed,

Chief Strategy Officer