STRATEGIC COUNTRY REPORT: MOROCCO

Automated Strategic Analyst (v2.2 Parallel)

12 February 2026

Contents

Chapter 1

Geopolitics

1.1 Geopolitics

Executive Summary

Morocco is currently executing a strategic pivot in its digital and geopolitical posture, moving away from an exclusive reliance on traditional European partnerships toward a diversified portfolio of alliances. This shift is characterized by a deepening integration with the United States and Israel, formalized through the Abraham Accords and the establishment of a trilateral investment fund aimed at financing strategic digital infrastructure [Source 2]. While Morocco maintains significant policy alignment with the European Union—evidenced by participation in the Global Gateway strategy and the Medusa submarine cable project—it is actively counterbalancing the regional trend where neighboring North African states are increasingly turning to China for trade and investment [Source 1]. Despite these diplomatic maneuvers to enhance resilience, Morocco's digital topology exhibits a critical technical vulnerability: a high degree of centralization in upstream connectivity. Analysis reveals that a single entity, Cloudflarenet, serves as a massive dependency for the national network, creating a potential single point of failure or "chokepoint" for the country's internet traffic [Internal Graph].

1.2 Strategic Realignment and Digital Alliances

Morocco's geopolitical strategy regarding digital infrastructure is defined by a deliberate effort to diversify partnerships beyond its historical ties to the European Union. While policy alignment with the EU remains high, economic interconnectivity has weakened, prompting Rabat to seek alternative strategic depth [Source 1]. A primary vector of this realignment is the trilateral investment fund involving the United States and Israel. Born from the Abraham Accords, this initiative leverages U.S. financial power and Israeli innovation to bolster Morocco's industrial and digital capabilities, positioning the Kingdom as a competitive hub in the Mediterranean and a stabilizer in the volatile Sahel region [Source 2].

This pivot occurs against a backdrop of intensified geopolitical competition in North Africa. While Morocco strengthens ties with the West and Israel, many of its neighbors are increasingly pivoting toward China as a "less demanding" partner for trade and investment [Source 1]. Morocco's strategy appears to be one of balancing: maintaining its status as a key partner in the EU's "Global Gateway" strategy—which aims to bridge the digital divide and foster sustainable digital economies—while simultaneously pursuing autonomy through diversification [Source 1] [Source 3]. Additionally, Morocco is leveraging soft power through digital and health diplomacy, evidenced by its $5 million pledge to Gavi, the Vaccine Alliance, positioning itself as a bridge between Africa and the global community [Source 2].

1.3 Infrastructure Diplomacy: The Physical Layer

Morocco's diplomatic ambitions are physically manifested in major submarine cable investments that reinforce its connectivity to Europe while attempting to project influence northward. A critical development is the **Medusa submarine cable project**, which interconnects Morocco, Algeria, Tunisia, and Egypt with five European nations (Portugal, Spain, France, Italy, and Cyprus). Supported by a €40 million EU grant under the Economic and Investment Plan for the Southern Mediterranean, and utilizing Nokia technology, this project underscores Morocco's continued physical integration with the European digital ecosystem [Source 2] [Source 5].

Further strengthening this link is the **Canalink-Morocco** project, financed under the CEF Digital program, designed to boost connectivity between Africa and Europe [Source 1]. However, Morocco's ambitions have faced setbacks. The **Xlinks** project, a massive $22 billion proposal to lay high-voltage submarine cables and fiber from Morocco to the United Kingdom, was intended to supply 8% of the UK's electricity. Recent intelligence indicates the UK has "snubbed" the plan regarding funding, highlighting the risks inherent in such high-stakes infrastructure diplomacy [Source 3] [Source 4].

At the corporate level, Morocco's telecom sector remains deeply intertwined with French interests. The participation of the Moroccan provider 'du' in the **Orange Alliance Program** grants it access to Orange's global platforms and governance expertise. While this fosters innovation and operational efficiency, it reinforces a degree of reliance on French telecommunications standards and infrastructure [Source 4].

1.4 Critical Digital Dependencies and Vulnerabilities

Beneath the diplomatic layer of diverse alliances, Morocco's logical internet topology reveals significant centralization risks. Intelligence analysis of the Autonomous System Numbers (ASNs) providing transit to Morocco identifies **Cloudflarenet** as the most significant upstream connectivity provider. With 956 other ASNs depending on it, Cloudflarenet represents a disproportionate percentage of Morocco's upstream connectivity. This concentration indicates a potential "chokepoint," where a technical failure or targeted action against this single entity could disrupt a vast portion of the nation's internet traffic [Internal Graph].

While other ASNs such as ASMedi (26 dependencies), IAM-AS (23 dependencies), and Maroc-connect (14 dependencies) provide some transit, they pale in comparison to the dominance of Cloudflarenet. Furthermore, hegemony analysis reveals that several local entities, including Enterprise-Services and UM6P-AS, exhibit a 100% dependency (Hegemony Score of 1.0) on specific central ASNs. This lack of upstream diversity contradicts the government's diplomatic strategy of diversification, suggesting that while Morocco is politically widening its circle of allies, its digital backbone remains technically constricted and vulnerable [Internal Graph].

References

- [Source 1] The EU's geopolitical dream is dying in its own neighbourhood (https://blogs.lse.ac.uk/europpb
eus-geopolitical-dream-is-dying-in-its-own-neighbourhood/)
- [Source 2] A blueprint for a trilateral Morocco-Israel-US investment fund (https://www.atlanticcouncil.org
blueprint-for-a-trilateral-morocco-israel-us-investment-fund/)
- [Source 3] International Partnerships - International Partnerships (https://international-partnerships.ec.europa.eu/index_en)
- [Source 4] du joins the Orange Alliance Program to strengthen collaboration ... (https://newsroom.orange.com/du-joins-the-orange-alliance-program-to-strengthen-collaboration-drive-innovation-and-accelerate-digital-transformation/)
- [Source 5] News & Articles - World Advanced Manufacturing Morocco 2026 (https://www.wammorocco.co
articles)
- [Internal Graph] IYP-GRAPH - Internal Intelligence Graph Data (Upstream Connectivity and ASN Analysis)

Chapter 2

Infrastructure

Executive Summary

Morocco's telecommunications infrastructure is characterized by a distinct dichotomy: a robust and rapidly expanding fixed fiber-optic sector contrasted with a nascent and delayed mobile 5G rollout. As of late 2024, the Kingdom has achieved significant milestones in Fiber to the Home (FTTH) penetration, driven by regulatory reforms aimed at increasing wholesale competition and infrastructure sharing [Source 1][Source 3]. However, the mobile sector lags behind regional peers, with 5G commercial deployment not expected to commence until late 2025 [Source 4].

From a strategic network topology perspective, Morocco's internet architecture exhibits high centralization. A single Autonomous System (MT-MPLS) controls over 60% of the network, creating a significant strategic chokepoint [IYP-GRAPH]. Furthermore, critical dependencies on external content delivery networks (specifically Cloudflare) and specific domestic ASNs (ASMedi and IAM-AS) indicate potential vulnerabilities in the event of targeted disruption or technical failure [IYP-GRAPH]. While the "Digital Morocco 2030" strategy outlines ambitious connectivity goals, the physical infrastructure currently suffers from notable rural coverage gaps, particularly in eastern and central regions, and demonstrated fragility during recent natural disasters [Source 2][Source 10].

2.1 Fixed Broadband and Fiber Optic Development

Morocco has prioritized the expansion of wired broadband infrastructure, resulting in a measurable shift toward high-speed fiber connectivity. As of the fourth quarter of 2024, FTTH penetration reached 38.5% of the wired broadband market, totaling approximately 990,000 connections [Source 3]. This infrastructure expansion has directly correlated with improved network performance; median fixed broadband download speeds rose by 32% year-on-year to 35.57 Mbps, while median upload speeds reached 31.86 Mbps, surpassing regional competitors such as Egypt [Source 3].

Despite these gains, the physical layout of the national fiber backbone remains opaque. Publicly available intelligence does not detail the specific routing or capacity of the backbone, though utility fiber networks are known to have coverage gaps compared to incumbent networks, specifically in the eastern and central regions of the country [Source 2]. To address these deficiencies, the government has implemented reforms to license carrier-neutral wholesale operators and mandate access to passive infrastructure (ducts and towers), aiming to lower investment costs for private sector actors [Source 1].

2.2 Mobile Network Evolution and 5G Readiness

Unlike its accelerated fiber deployment, Morocco's transition to next-generation mobile infrastructure is currently in the planning phase. There is no active commercial 5G population coverage. The projected timeline for 5G rollout is as follows: * **Initial Limited Launch:** Scheduled for announcement in Q3 2025. * **Coverage Targets:** 25% population coverage by the end of 2026, reaching 70% by 2030 [Source 4].

Intelligence regarding the enabling environment for this rollout is limited. There is no definitive information available regarding the outcomes of recent spectrum auctions or the specific frequency bands allocated for 5G services [Source 4][Source 5]. This lack of transparency regarding spectrum availability raises questions about the capacity of local operators to support future high-capacity mobile demands. Furthermore, while the "Digital Morocco 2030" strategy emphasizes connectivity, it acknowledges a persistent digital divide, with approximately 1,800 rural villages currently lacking internet access [Source 11].

2.3 Network Topology and Strategic Chokepoints

Analysis of Morocco's logical network infrastructure reveals a highly concentrated ecosystem dominated by a few key entities. The network is heavily reliant on **MT-MPLS**, which accounts for approximately 61.85% of the network's reach. **ASMedi** follows with 30.79%, while **IAM-AS** holds 6.21% [IYP-GRAPH]. This distribution indicates that MT-MPLS acts as the primary backbone for national traffic, representing a single point of failure for the majority of the country's internet connectivity.

Critical Dependencies: * **Cloudflare (CLOUDFLARENET):** Identified as a significant chokepoint with 956 incoming dependencies. The high volume of reliance on this single entity suggests that a disruption to Cloudflare's services would have a disproportionate impact on Moroccan digital services [IYP-GRAPH]. * **Domestic Interconnectivity:** ASMedi (130 dependencies) and IAM-AS (115 dependencies) serve as critical nodes for connecting other domestic networks and data centers. Analysis indicates that entities such as Enterprise-Services and Maroc-Datacenter-MDC exhibit 100% dependency on specific upstream ASNs (e.g., ASN 36925), highlighting a lack of redundancy in upstream connectivity for critical facilities [IYP-GRAPH]. * **Traffic Exchange:** Cloudflare exhibits extensive Internet Exchange Point (IXP) membership (1057 memberships), facilitating local traffic retention. In contrast, the Moroccan Academic & Research WAN (MARWAN-AS) shows minimal IXP participation, suggesting its traffic is more likely to egress internationally, potentially increasing latency and exposure to foreign surveillance [IYP-GRAPH].

2.4 Infrastructure Resilience and Physical Security

The resilience of Morocco's telecommunications infrastructure is a concern, particularly in the context of natural disasters. Following the 2023 earthquake, damaged infrastructure significantly hampered rescue efforts, exposing the fragility of communication lines in rugged terrain [Source 10]. While specific disaster recovery plans for fiber and tower restoration are not publicly detailed, the geographic gaps in the fiber backbone in eastern and central Morocco exacerbate the risk of communication blackouts in those areas during crises [Source 2].

Furthermore, there is a lack of verifiable intelligence regarding the physical readiness of Moroccan data centers to support advanced computing needs (AI/Cloud). No major hyperscale or colocation facilities with certified Tier ratings have been identified in open-source intelligence, and assessments of power and cooling infrastructure for future capacity growth are currently unavailable [Source 8].

References

- [Source 1] High Speed Internet Infrastructure in Morocco – Key Reforms (https://documents.worldbank.or Speed-Internet-Infrastructure-in-Morocco-Key-Reforms.pdf)
- [Source 2] Broadband Networks in the Middle East and North Africa - World Bank (https://www.worldbank.org/content/dam/Worldbank/document/MNA/Broadband_report/Broadband
- [Source 3] Fiber Brings Faster Fixed Broadband to North Africa with ... - Ookla (https://www.ookla.com/articles/fixed-speeds-north-africa-2024)
- [Source 4] Morocco - Telecommunications - International Trade Administration (https://www.trade.gov/country-commercial-guides/morocco-telecommunications)
- [Source 5] Iliad's market entry and the 5G spectrum auction - Analysys Mason (https://www.analysysmason.com/about-us/news/newsletter/iliads-market-entry-5g-spectrum-apr2019/)
- [Source 6] Digitalisation and the Africa We Want - GSMA Intelligence (https://www.gsmaintelligence.com file-download?reportId=50173&assetId=7701)
- [Source 7] Digital dividend: Insights for spectrum decisions - ITU (https://www.itu.int/en/ITU-D/Spectrum-Broadcasting/Documents/Publications/DigitalDividend_Final_2018.pdf)
- [Source 8] ABB powers Philippines' first AI-ready hyperscale data center with ... (https://new.abb.com/news/detail/131355/abb-powers-philippines-first-ai-ready-hyperscale-data-center-with-resilient-sustainable-infrastructure?utm_source=linkedin&utm_medium=p ai-ppc-promo&utm_content=video)
- [Source 9] List of Internet exchange points - Wikipedia (https://en.wikipedia.org/wiki/List_of_Internet_
- [Source 10] Q&A: Achref Chibani on Climate Change, Natural Disasters, and ... (https://www.wilsoncenter.org/article/qa-achref-chibani-climate-change-natural-disasters-

and-building-resilience-libya-and)

- [Source 11] Morocco - Digital Economy - International Trade Administration (https://www.trade.gov/country-commercial-guides/morocco-digital-economy)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 3

Market

Executive Summary

The Moroccan telecommunications market is characterized by a highly concentrated, rigid oligopoly dominated by three primary operators: Maroc Telecom (IAM), Orange Morocco, and Inwi. As of 2024, the market exhibits a distinct divergence between subscriber volume and revenue generation; while Inwi has secured the largest share of mobile subscribers, the incumbent Maroc Telecom retains the dominant position in revenue market share, suggesting superior pricing power and a higher-value customer base [Source 1][Source 3].

Market concentration metrics indicate a lack of significant competition, with a Herfindahl-Hirschman Index (HHI) score well above the threshold for a highly concentrated market [Source 2]. Infrastructure development remains robust, with Morocco ranking second in North Africa for fixed broadband performance and operators collaborating on fiber and 5G deployment [Source 2][Source 4]. However, the sector lacks a "disruptor" entity capable of forcing aggressive price corrections, leading to consumer sentiment regarding inflated pricing despite the country meeting United Nations affordability targets [Source 5][Source 6].

3.1 Market Structure and Competitive Landscape

The Moroccan mobile market is split nearly evenly among three operators, creating a fiercely contested but static environment. As of 2024, Inwi holds the leading subscriber market share at 35.3%, followed closely by Maroc Telecom at 32.5% and Orange Morocco at 32.3% [Source 2].

Despite the parity in subscriber numbers, the market is mathematically defined as "highly concentrated." The Herfindahl-Hirschman Index (HHI) for the sector is estimated at 3345.63, significantly surpassing the 2500 threshold that regulators typically associate with high concentration and reduced competitive intensity [Source 2].

A critical disparity exists between subscriber volume and financial performance. While Inwi leads in user count, Maroc Telecom commands the highest revenue market share at 36.1%, generating approximately USD $3.67 billion in consolidated revenue in 2024 [Source 1]. Orange Morocco follows with 32.9% of revenue, and Inwi trails with 31% [Source 1]. This revenue dominance by the incumbent, despite a lower subscriber count than Inwi, indicates strong monetization strategies and a potential stronghold on the enterprise or post-paid segments.

3.2 Infrastructure and Network Performance

Morocco maintains a competitive infrastructure position relative to its regional peers. In the fixed broadband segment, the country ranked second in North Africa for performance in Q4 2024 [Source 4]. Network speed analysis indicates a median fixed broadband download speed of 35.57 Mbps (Q4 2024) and a median upload speed of 31.86 Mbps (Q3 2022), the latter of which allowed Morocco to overtake Egypt in regional rankings [Source 4].

To sustain infrastructure growth, operators are engaging in strategic partnerships. Notably, Maroc Telecom and Inwi have partnered to accelerate the deployment of fiber optics and 5G technology, signaling a cooperative approach to capital-intensive infrastructure upgrades rather than purely competitive infrastructure duplication [Source 2].

3.3 Pricing Dynamics and Affordability

The affordability of mobile data in Morocco has improved, with the country meeting the United Nations' affordability target—where 1GB of data costs no more than 2% of average monthly income—for the first time in 2020 [Source 5].

However, the market lacks a significant "disruptor" operator (similar to Free in France) that utilizes aggressive pricing strategies or innovative bundling to destabilize established pricing structures [Source 7]. Consequently, open-source intelligence suggests growing consumer dissatisfaction regarding perceived price alignment among the three major ISPs. User sentiment indicates concerns that despite shared infrastructure and mature networks, pricing remains inflated, with limited variation in service costs between operators [Source 6][Source 8].

References

- [Source 1] Morocco - Telecommunications - International Trade Administration (https://www.trade.gov/country-commercial-guides/morocco-telecommunications)
- [Source 2] Maroc Telecom, Inwi partner to deploy fiber and 5G (https://www.connectingafrica.com/connec telecom-inwi-partner-to-deploy-fiber-and-5g)
- [Source 3] Morocco Telecom Operators Country Intelligence Report - GlobalData (https://www.globaldata.com/store/report/morocco-telecom-operators-market-analysis/)
- [Source 4] Fiber Brings Faster Fixed Broadband to North Africa with ... - Ookla (https://www.ookla.com/articles/fixed-speeds-north-africa-2024)
- [Source 5] Mobile data costs fall but as demand for internet services surges ...

(https://webfoundation.org/2021/03/mobile-data-costs-fall-but-as-demand-for-internet-services-surges-progress-remains-too-slow/)

- [Source 6] Internet prices in Morocco - Reddit (https://www.reddit.com/r/Morocco/comments/18gjr9h/in
- [Source 7] Softbank's disruptive pricing transforms Japan's mobile market (https://www.gsmaintelligence.
disruptive-pricing-transforms-japans-mobile-market-aggressive-pricing-stealing-thunder-from-docomo-kddi)
- [Source 8] inflated Internet prices : r/Morocco - Reddit (https://www.reddit.com/r/Morocco/comments/1
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 4

Localization

Executive Summary

Morocco is currently navigating a complex transition between rapid digital transformation and the strategic imperative of data sovereignty. Under the "Digital Morocco 2030" vision, the Kingdom is actively modernizing its public administration and economy, yet it remains heavily reliant on foreign hyperscale cloud providers for critical infrastructure [Source 10, Source 15]. While the government has established a legal framework for data protection (Law 09-08) and cybersecurity (Law 05-20) to regulate data handling and critical infrastructure [Source 13, Source 16], there is a notable absence of domestic hyperscale cloud regions. Consequently, a significant portion of national data is likely hosted in foreign jurisdictions, exposing Moroccan entities to extraterritorial legal risks such as the U.S. Cloud Act [Source 4]. The Kingdom is pursuing a "Sovereign Cloud" strategy to mitigate these risks, but specific milestones and the ratio of local-to-foreign hosting remain opaque [Source 10].

4.1 Cloud Infrastructure and Market Dynamics

The Moroccan cloud market mirrors global trends, characterized by the dominance of major foreign hyperscalers. While specific market share data for Morocco is unavailable, global metrics indicate that Amazon Web Services (AWS), Microsoft Azure, and Google Cloud collectively control approximately 64% of the public cloud market [Source 1]. This oligopoly extends to the African continent, where AWS has identified Morocco as a target for future infrastructure deployment, although no full-scale data center region has been established in the country to date [Source 6].

The reliance on foreign infrastructure is further entrenched by international partnerships. The U.S. Trade and Development Agency (USTDA) actively connects Moroccan decision-makers with U.S. technology providers for data center and e-government solutions [Source 7]. This dynamic suggests that while local hosting providers exist, they face significant competition from global entities that offer advanced scalability and services. The absence of granular data on local versus foreign market share represents a significant intelligence gap, obscuring the precise extent of foreign dependency [Source 1].

4.2 Data Sovereignty and Legal Framework

Morocco has developed a robust legislative architecture to govern data localization and security, though enforcement challenges persist regarding cross-border data flows.

Legislative Instruments: The primary instrument for data privacy is the Personal Data Protection Law (Law No. 09-08), overseen by the National Commission for the Protection of Personal Data (CNDP). This law stipulates conditions for transferring data abroad [Source 13, Source 16]. Additionally, the Cybersecurity Law (Law No. 05-20) and the subsequent Decree on Critical Infrastructure Security (July 2021) mandate that critical infrastructure providers classify information systems and adhere to security rules established by the General Directorate of Information Systems Security (DGSSI) [Source 13, Source 16].

Extraterritorial Risks: Despite domestic protections, the hosting of data on foreign cloud platforms subjects Moroccan data to extraterritorial jurisdiction. The U.S. Cloud Act allows U.S. law enforcement to access data held by U.S. service providers regardless of the data's physical location [Source 4]. This creates a compliance paradox for Moroccan entities, who must navigate local data residency requirements while utilizing foreign infrastructure that may not guarantee immunity from foreign government access [Source 4].

Sovereign Cloud Strategy: To counter these risks, the "Digital Morocco 2030" strategy explicitly outlines a move toward a "Sovereign Cloud." This initiative aims to enhance national security by ensuring controlled data handling and fostering local digital talent [Source 10]. However, the strategy currently lacks public milestones or specific targets for repatriating data from foreign servers [Source 10, Source 12].

4.3 E-Government Hosting and Domain Localization

Public Service Infrastructure: Morocco's e-government evolution involves a hybrid approach to infrastructure. While the government aims for a unified portal under its digital strategy, there is documented reliance on foreign technology stacks. For instance, government agencies have modernized critical systems using IBM WebSphere Liberty and IBM LinuxONE to enhance data sharing and security, indicating that the underlying architecture of some sovereign services is dependent on non-domestic technology providers [Source 8].

Domain Name (.ma) Adoption: The management of the country's top-level domain, .ma, is a component of its digital localization. Registration for .ma domains is generally unrestricted, but strict localization rules apply to administrative contacts, who must be located within Morocco [Source 17]. Furthermore, specific subdomains such as .gov.ma are restricted, implying a policy of identifying and segregating official government digital assets [Source 17]. However, intelligence on the adoption rate of .ma compared to generic domains like .com is limited, with regional studies suggesting that cost and infrastructure challenges often drive African entities toward offshore legacy gTLDs [Source 2, Source 3].

References

- [Source 1] Public cloud revenue: Spending boom for AWS, Azure and Google ... (https://www.techmonitor.ai/cloud/public-cloud-revenue-aws-azure-google-cloud/)
- [Source 2] Middle East and Adjoining Countries DNS Study | ICANN (https://www.icann.org/en/system/ dns-study-26feb16-en.pdf)
- [Source 3] Five Years of Africa Strategy Implementation - icann (https://www.icann.org/en/system/files/f strategy-implementation-2012-2017-03may18-en.pdf)
- [Source 4] Where is Africa in the cloud? | NTU Singapore (https://www.ntu.edu.sg/cas/news-events/news/details/where-is-africa-in-the-cloud)
- [Source 5] Public Cloud Regions and Data Centers | Oracle (https://www.oracle.com/cloud/public-cloud-regions/)
- [Source 6] AWS Bets on Africa’s Fast-Growing Cloud Market - Ecofin Agency (https://www.ecofinagency.com/telecom/3004-46712-aws-bets-on-africa-s-fast-growing-cloud-market)
- [Source 7] USTDA Supports Morocco’s Digital Transformation (https://www.ustda.gov/ustda-supports-moroccos-digital-transformation/)
- [Source 8] Government agency in Morocco through PowerM - IBM (https://www.ibm.com/case-studies/govt-dept-in-morocco)
- [Source 9] Morocco - Digital Economy - International Trade Administration (https://www.trade.gov/count commercial-guides/morocco-digital-economy)
- [Source 10] Sovereign Cloud for Government Agencies in Middle East - Cloud4C (https://www.cloud4c.com/blogs/sovereign-cloud-transformations-in-middle-east)
- [Source 11] Interconnection and Traffic exchange towards 80% locally accessed ... (https://www.internetsociety.org/wp-content/uploads/2017/08/Brochure_-_Interconnection_and_Traffi
- [Source 12] 2025 State of the Cloud Report - Flexera (https://info.flexera.com/CM-REPORT-State-of-the-Cloud?lead_source=Organic%20Search)
- [Source 13] 2024 Investment Climate Statements: Morocco (https://www.state.gov/reports/2024-investment-climate-statements/morocco)
- [Source 14] 2025 Investment Climate Statements: Morocco (https://www.state.gov/reports/2025-investment-climate-statements/morocco)
- [Source 15] Morocco - United States Department of State (https://2021-2025.state.gov/reports/2023-investment-climate-statements/morocco/)
- [Source 16] DPA Digital Digest: Morocco [2025 Edition] (https://digitalpolicyalert.org/digest/dpa-digital-digest-morocco)
- [Source 17] WIPO Domain Name Dispute Resolution Service for .MA and . (https://www.wipo.int/amc/en/domains/cctld/ma/index.html)
- [Source 18] Cross-Border Data Regulatory Frameworks (https://ir.lawnet.fordham.edu/iplj/vol34/iss4/2/

- [Source 19] New Standard Contractual Clauses - Questions and Answers overview (https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 5

Security

Executive Summary

Morocco exhibits a distinct dichotomy between its high-level strategic governance and its operational technical security posture. Strategically, the nation has established itself as a regional leader in cybersecurity governance, achieving “Tier 1” status in the 2024 ITU Global Cybersecurity Index with a score of 97.5/100 [Source 1]. This ranking is underpinned by robust legal frameworks, capacity-building measures, and the active involvement of institutions such as the General Directorate for Information Systems Security (DGSSI) and maCert.

However, technical intelligence reveals significant vulnerabilities within the national internet infrastructure. Despite strong governance scores, the operational layer suffers from a critical lack of security hygiene. Notably, there is a complete absence of DNSSEC adoption across the top 10 Autonomous System Numbers (ASNs) by population reach, including the dominant provider MT-MPLS [IYP-GRAPH]. Furthermore, the network topology is characterized by high centralization and “chokepoints,” where critical entities exhibit 100% dependency on single upstream providers, creating systemic risks for national connectivity [IYP-GRAPH]. While specific data on malware infection rates is limited, the broader regional context suggests a rising threat landscape driven by increasing cybercriminal sophistication across Africa [Source 3].

5.1 Strategic Governance and Global Standing

Morocco has successfully positioned itself as a cybersecurity leader within the African and Arab regions. The nation’s commitment to cyber resilience is reflected in its ranking of 30th globally on the National Cyber Security Index (NCSI) [Source 4]. This standing is driven by a comprehensive approach to cyber defense, which includes:

- **Legal and Organizational Frameworks:** Morocco scored a full 20 points in the “Legal, Organizational, and Cooperation Measures” sub-category of the ITU GCI [Source 1]. This indicates a mature legislative environment capable of addressing cybercrime and regulating digital security.

- **Capacity Building:** The country achieved 19.38 points in capacity building, highlighting effective training programs, awareness campaigns, and the development of human capital in the cyber domain [Source 1].
- **Institutional Oversight:** The ecosystem is supported by active monitoring centers like maCert and the strategic direction of the DGSSI, which facilitate international cooperation and incident response [Source 1].

5.2 Network Topology and Critical Infrastructure Vulnerabilities

Intelligence regarding Morocco's internet topology indicates a highly centralized structure with significant dependencies that could serve as single points of failure.

- **Chokepoint Analysis:** Analysis of downstream dependencies identifies IAM-AS (Maroc Telecom) as a critical chokepoint with significant incoming dependencies. Additionally, Cloudflare-related ASNs (CLOUDFLARENET) exhibit an exceptionally high number of incoming dependencies (956), suggesting that a vast portion of the national digital infrastructure relies on this single provider for connectivity and security services [IYP-GRAPH].
- **High Interdependency:** Network telemetry reveals that several critical ASNs, including academic and government-related entities such as UM6P-AS, Maroc-Datacenter-MDC, and Enterprise-Services, exhibit 100% dependency (hegemony) on central ASNs like 36925 and 36884. This high level of centralization means that misconfiguration or compromise of these central nodes could result in immediate, large-scale service disruptions for dependent networks [IYP-GRAPH].

5.3 Technical Security Hygiene

Despite the strong policy framework, the implementation of technical security protocols at the network layer remains a critical weakness.

- **DNSSEC Adoption:** There is a confirmed lack of Domain Name System Security Extensions (DNSSEC) implementation among the country's most critical networks. All top 10 ASNs by population reach—including MT-MPLS (61.85% reach), ASMedi (30.79%), and IAM-AS (6.21%)—report zero DNSSEC adoption [IYP-GRAPH]. This leaves the majority of Moroccan internet users vulnerable to DNS spoofing and cache poisoning attacks.
- **Routing Security (RPKI/MANRS):** While specific validation rates are unavailable, the high dependency scores of major ASNs (e.g., HOSTOWEB, MARWAN-AS) combined with the lack of confirmed RPKI validation suggests a fragility in the routing infrastructure. The centralization of traffic through nodes with unverified routing security postures increases the risk of BGP hijacking events propagating rapidly through the national network [IYP-GRAPH].

5.4 Threat Landscape

The cyber threat landscape facing Morocco is influenced by broader regional trends. While specific telemetry on botnet origins within Morocco is currently unavailable, the *Interpol African Cyberthreat Assessment Report 2022* highlights a continent-wide increase in cyber threats [Source 3]. Key factors contributing to this risk profile include:

- **Digital Literacy Gaps:** Challenges regarding digital literacy contribute to a user base that is more susceptible to social engineering and phishing attacks [Source 3].
- **Regional Cybercrime:** The sophistication of cybercriminals operating within the African continent is increasing, leveraging weak legal frameworks in neighboring jurisdictions to launch attacks [Source 3].

References

- [Source 1] Morocco has improved its position in the Global Cybersecurity Index (https://www.dgssi.gov.ma/en/actualites/morocco-has-improved-its-position-global-cybersecurity-index-recently-published)
- [Source 2] Global Cybersecurity Index 2024 - ITU (https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf)
- [Source 3] AFRICAN CYBERTHREAT ASSESSMENT REPORT ... - Interpol (https://www.interpol.int/content/download/19174/file/2023_03%20CYBER_African%20Cyberthreat%
- [Source 4] Update of the National Cyber Security Index (NCSI) - | DGSSI (https://www.dgssi.gov.ma/en/a jour-du-national-cyber-security-index-ncsi)
- [IYP-GRAPH] Internal Knowledge Graph (Network Telemetry & Topology Analysis)

Chapter 6

Governance

Executive Summary

Morocco's governance of the digital and telecommunications sectors is characterized by a dualistic strategy: a drive toward economic modernization and regulatory alignment with European standards, juxtaposed against a rigid state security apparatus that retains extensive surveillance and censorship capabilities. While the Kingdom has established the National Commission for the Protection of Personal Data (CNDP) and enacted Law No. 09-08 to harmonize with the EU's General Data Protection Regulation (GDPR) `[Source 2, Q5]`, these protections are frequently circumvented by national security imperatives.

Intelligence indicates that Morocco has not ratified the Malabo Convention, limiting its integration into the African Union's continental cybersecurity framework `[Source 2, Q2]`. Domestically, the state maintains a monopoly on the legitimate use of encryption and leverages "red lines"—criticism of the Monarchy, Islam, or Territorial Integrity—to justify the surveillance of dissidents and the blocking of online content `[Source 3, Q6]`. The telecommunications regulator, ANRT, possesses the legal authority to enforce market rules but operates within a political environment that historically favors the incumbent, Maroc Telecom `[Source 2, Q8]`. Consequently, the governance model prioritizes regime stability and state control over unbridled digital freedom.

6.1 Legal Framework and International Commitments

Morocco's approach to international cyber governance demonstrates a hesitation to bind itself to regional multilateral frameworks. The Kingdom has **not ratified** the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). This non-ratification limits Morocco's participation in the continental framework for cybersecurity cooperation, distinguishing it from other regional powers that have engaged with the treaty `[Source 2, Q2]`. Furthermore, while the Budapest Convention on Cybercrime is a key international instrument, there is no confirmation of Morocco's ratification in current intelligence holdings, potentially limiting its formal channels for mutual legal assistance in cybercrime cases [Source 1, Q2].

Domestically, the primary legislative instrument for privacy is **Law No. 09-08** (2009), which established the CNDP. The law aims to protect individuals against data misuse and aligns Morocco's framework with European partners to facilitate economic integration [Source 3, Q5]. However, the application of this law regarding state surveillance remains opaque. While the law protects citizens from commercial misuse, it does not explicitly detail limitations on state intelligence gathering [Source 3, Q5].

Regarding cryptography, the state maintains strict control. The import, export, supply, or use of encryption technologies requires prior declaration or authorization from the Directorate General for Information Systems Security (DGSSI). Non-compliance is a criminal offense punishable by imprisonment [Source 2, Q10].

6.2 Telecommunications Regulation and Market Oversight

The telecommunications sector is regulated by the **Agence Nationale de Réglementation des Télécommunications (ANRT)**, established under Law No. 24-96 [Source 2, Q1]. The ANRT is funded through administrative fees and holds the authority to sanction operators [Source 2, Q1]. This enforcement capability was demonstrated when the agency fined the dominant market player, Maroc Telecom, approximately $6.4 million for anti-competitive practices [Source 3, Q1].

Despite the regulatory framework, the market retains characteristics of its monopolistic past. Maroc Telecom, the former state-owned enterprise, continues to hold a dominant position, historically controlling over 90% of the ISP market share [Source 2, Q8]. While the licensing framework under Law 24-96 and subsequent amendments (Law 55-01) aims to foster competition and universal service, the transition has been gradual. Historical data suggests that high access costs and the incumbent's dominance have previously hindered broader internet penetration [Source 2, Q8].

6.3 Surveillance, Censorship, and Digital Rights

The governance of digital rights in Morocco is marked by significant state overreach and a lack of judicial oversight.

Surveillance and Privacy The legal framework governing state surveillance lacks transparency. Authorities are reported to access devices and data without clear warrant requirements or due process [Source 2, Q7]. Intelligence reports confirm that the government has monitored private online communications without appropriate legal authority [Source 1, Q3]. High-profile dissidents and journalists, such as Fouad Abdelmoumni, have been targeted using NSO Group's **Pegasus spyware**, creating a chilling effect on freedom of association and expression [Source 1, Q4]. Domestic oversight bodies like the CNDP have failed to provide effective remedies for these privacy violations [Source 1, Q4].

Censorship and Content Control The state actively filters and blocks content deemed threats to "public order" or the Kingdom's "sacred values." * **Legal Basis:** The Penal Code and Antiterrorism Act are utilized to prosecute online speech. "Red lines" include criticism of the King, Islam, or the Western Sahara issue (territorial integrity) [Source 3, Q6]. * **Blocking Incidents:** Documented cases include the blocking of news outlet *Lakome.com* and the arrest of its editor, as well as the blocking of the *Algeria Press Service* (APS) [Source 1, Q6]. * **Internet Disruptions:** The U.S. Department of State has reported government-initiated disruptions to internet access [Source 1, Q3].

Draft legislation, such as Law No. 22.20, has previously proposed granting network providers broad powers to restrict content threatening "public order," further indicating a policy trajectory favoring state control over open access [Source 2, Q6].

References

International Treaties & Legal Framework * [Source 1, Q2] THE MALABO ROADMAP - Data Protection Africa (https://dataprotection.africa/wp-content/uploads/malabo_roadmap_Sept_2022.pdf) * [Source 2, Q2] Africa's Cybersecurity Treaty Enters into Force - directions blog (https://directionsblog.eu/africas-cybersecurity-treaty-enters-into-force/) * [Source 3, Q5] Law No. 09-08 on the protection of individuals with regard to the processing of personal data (https://www.dgssi.gov.ma/en/loi-09-08-relative-la-protection-des-personnes-physiques-legard-du-traitement-des) * [Source 2, Q5] Moroccan data protection law: Moving to align with EU data protection (https://iapp.org/news/a/moroccan-data-protection-law-moving-to-align-with-eu-data-protection) * [Source 2, Q10] Countries with Encryption Restrictions (https://www.umassp.edu/sites/default/files/publications/encryption-restriction-countries_final-011025.pdf)

Telecommunications & ANRT * [Source 2, Q1] Authorization process for independent radio networks (IRN) - ANRT (https://www.anrt.ma/en/accordeon/authorization-process-independent-radio-networks-irn) * [Source 3, Q1] 2025 Investment Climate Statements: Morocco (https://www.state.gov/reports/2025-investment-climate-statements/morocco) * [Source 2, Q8] The Impact of Liberalizing the Telecommunication Sector in Morocco (https://mpra.ub.uni-muenchen.de/8675/1/telecom-paper-Morocco.pdf)

Surveillance, Censorship & Human Rights * [Source 1, Q4] Amicus Brief in NSO Group Technologies Ltd. et al. (https://www.accessnow.org/wp-content/uploads/2020/12/2020-12-22-AccessNow-Amicus-Brief13845453.1.pdf) * [Source 2, Q7] EXPANSION OF DIGITAL SURVEILLANCE AND IMPACTS (https://www.ohchr.org/sites/default/files/documents/issues/civicspace/re space-tech-brief-surveillance-trends-middle-east-north-africa-1-en.pdf) * [Source 1, Q3/Q9] Morocco - United States Department of State (2023 Country Reports on Human Rights Practices) (https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/morocco) * [Source 1, Q6] Internet censorship in Morocco - Wikipedia (https://en.wikipedia.org/wiki/Internet_censorship_ * [Source 2, Q6] Morocco: Government must fully withdraw draft law on social media

(https://menarights.org/en/articles/morocco-government-must-fully-withdraw-draft-law-social-media) * [Source 3, Q6] Will Morocco Regulate the Internet? An Interview with Zineb Belmkaddem (https://www.eff.org/deeplinks/2013/12/will-morocco-regulate-internet-interview-zineb-belmkaddem-and-ibn-kafka)

Chapter 7

Strategic Synthesis & Roadmap

Chapter 8

Section 7: Strategic Synthesis & Roadmap

To: The Head of State **From:** Office of the Chief Strategy Officer **Date:** October 26, 2025 **Subject:** The “Glass Fortress” – Reconciling Geopolitical Ambition with Digital Fragility

---

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

8.1.1 The Narrative: The Gateway Strategy

Your Excellency, Morocco is successfully executing a geopolitical pivot. By diversifying alliances beyond the EU to include the United States and Israel, and by positioning the Kingdom as the physical landing point for trans-Atlantic and Mediterranean data cables (Medusa, Canalink), we are effectively marketing Morocco as the **“Digital Gateway to Africa.”** We are selling stability and connectivity in a volatile region.

8.1.2 The Paradox: The “Glass Fortress”

However, a critical contradiction threatens this vision. We have built a **diplomatic fortress** on a **digital glass floor**. While our foreign policy aggressively seeks diversification to ensure resilience, our technical infrastructure has quietly slid into extreme centralization. * **Diplomatically**, we have many allies. * **Technically**, we rely on a single digital lung. Intelligence reveals that a massive percentage of our national traffic relies on a single upstream provider (Cloudflarenet) and a single domestic backbone (MT-MPLS). If this “chokepoint” is squeezed—whether by technical error, cyberattack, or foreign sanction—our geopolitical leverage vanishes instantly. We have world-class cybersecurity *laws* (Tier 1 Global Index), but our operational *hygiene* is failing (Zero DNSSEC adoption on critical networks).

The Bottom Line: We are projecting power, but we are technically vulnerable to a single switch-flip.

8.2 2. SWOT Analysis: The Strategic Cheat Sheet

STRENGTHS (Internal)	WEAKNESSES (Internal)
Geographic Gravity: We are the physical intersection of the Atlantic and Mediterranean cable systems. **Fiber Maturity:** High FTTH penetration (38.5%) outperforms regional peers like Egypt. **Regulatory Framework:** Tier 1 Global Cybersecurity Index score; robust data protection laws (CNDP).	**The "Chokepoint":** Extreme reliance on Cloudflare and Maroc Telecom (MT-MPLS) creates a Single Point of Failure. **Security Hygiene:** Zero DNSSEC adoption on top networks leaves citizens vulnerable to spoofing. **5G Lag:** No commercial 5G coverage puts us behind the innovation curve for Industry 4.0.

OPPORTUNITIES (External)	THREATS (External)
"Nearshoring" 2.0: EU companies are leaving volatile Asian markets; we can capture their digital operations if our cloud is sovereign. **Energy-Digital Nexus:** Leveraging our renewable energy to power AI Data Centers (Green Compute). **West African Hegemony:** Exporting our banking/telecom stack to the Sahel as a stabilization tool.	**The Cloud Act:** Our data resides on US/EU servers, subject to foreign subpoenas, nullifying our sovereignty laws. **Regional Cyberwar:** Rising cybercrime in Africa and tensions with neighbors could exploit our routing centralization. **Digital Divide:** The gap between fiber-connected cities and unconnected rural villages risks social unrest.

8.3 3. Strategic Roadmap: The Policy Agenda

8.3.1 Phase 1: Immediate Stabilization (Months 1-6)

Goal: Secure the Perimeter & Fix Hygiene (Low Cost / High Impact)

1. **Executive Decree on Digital Hygiene:** Mandate **DNSSEC adoption** and **RPKI validation** for all Critical Information Infrastructure (CII) operators (Maroc Telecom, Inwi, Orange) and government domains (.gov.ma) within 90 days.
   - *Why:* We cannot be a digital hub if our directory system is spoofable. This costs political capital, not budget.
2. **The "Sovereign Routing" Directive:** Order the DGSSI to audit government dependency on Cloudflare. Mandate a **multi-vendor upstream strategy** for all sovereign services (Defense, Interior, Finance).

- *Why:* We must eliminate the single point of failure. If Cloudflare goes down, the State must stay up.

3. **Data Residency Audit:** Immediate classification of government data. "Top Secret" and "Secret" data must be repatriated from foreign hyperscalers (AWS/Azure) to on-premise government servers immediately.

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

Goal: Market Liberalization & Infrastructure Hardening

1. **Accelerate 5G Licensing with "Coverage Covenants":** Launch the 5G spectrum auction immediately, but attach strict "use-it-or-lose-it" clauses requiring rural coverage to prevent a digital divide.
   - *Why:* We are late. We need to leapfrog to catch up with global industry standards.
2. **Break the Oligopoly:** Empower the ANRT to enforce **Local Loop Unbundling** aggressively. If the incumbents (IAM/Orange/Inwi) refuse to lower wholesale prices, license a fourth "Wholesale-Only" infrastructure provider to spark competition.
3. **The "Green Cloud" Initiative:** Offer tax incentives for hyperscalers (Microsoft, Google) to build **physical data centers in Morocco**, strictly on the condition they are powered by our renewable energy sector.
   - *Why:* This solves the "Data Sovereignty" issue (data stays on our soil) and monetizes our green energy.

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

Goal: Regional Hegemony & Digital Sovereignty

1. **The "Atlas Cloud" Strategy:** Develop a domestic sovereign cloud capability (public-private partnership with UM6P) to host sensitive data for Morocco and our West African allies.
   - *Why:* We should be the "Digital Switzerland" of Africa—neutral, secure, and sovereign.
2. **Digital Diplomacy Export:** Export our DGSSI cybersecurity framework and ANRT regulatory model to Sahelian nations.
   - *Why:* Integrating their digital governance with ours creates a sphere of influence more powerful than military aid.

8.4 4. Final Verdict

8.4.1 Investability Score: HIGH

Explanation: Despite the market concentration, Morocco represents the most stable, fiber-connected entry point into Africa. The "Glass Fortress" risks are solvable with policy will. For investors, the convergence of Green Energy and Digital Infrastructure (cables/data centers) is a unique value proposition not found elsewhere in the region.

8.4.2 Maturity Score: DEVELOPING (High-Potential)

Explanation: We are “Mature” in fixed infrastructure and regulation, but “Emerging” in mobile (5G) and cloud sovereignty. We have the skeleton of a digital superpower, but we lack the muscle (local cloud) and the immune system (cyber hygiene).

Recommendation: Proceed with the 5G auction immediately, but prioritize the **Executive Decree on Digital Hygiene** as the first act of business. We cannot build a skyscraper on a cracked foundation.