STRATEGIC COUNTRY REPORT: TUNISIA

Automated Strategic Analyst (v2.2 Parallel)

03 February 2026

Contents

1 Geopolitics **3**
Executive Summary . . . 3
1.1 Geopolitical Alignment and Strategic Positioning . . . 3
1.2 Submarine Infrastructure and Regional Connectivity . . . 4
1.3 Digital Sovereignty and Network Vulnerabilities . . . 4
References . . . 5

2 Infrastructure **7**
Executive Summary . . . 7
2.1 Mobile and Fixed Network Architecture . . . 7
2.2 International Connectivity and Submarine Cables . . . 8
2.3 Network Topology and Critical Dependencies . . . 8
2.4 Internet Exchange Points (IXPs) and Peering . . . 9
2.5 Data Center and Cloud Infrastructure . . . 9
References . . . 9

3 Market **11**
Executive Summary . . . 11
3.1 Market Structure and Competitive Landscape . . . 11
3.2 Pricing and Affordability Analysis . . . 12
3.3 Network Infrastructure and Performance . . . 12
References . . . 12

4 Localization **14**
Executive Summary . . . 14
Regulatory Framework and Enforcement . . . 14
Digital Sovereignty and Infrastructure Maturity . . . 15
Public Sector Security and E-Government . . . 15
References . . . 15

5 Security **16**
Executive Summary . . . 16
5.1 National Cybersecurity Posture and Governance . . . 16
5.2 Network Infrastructure and Routing Security . . . 17
5.3 Threat Landscape: DDoS and Volumetric Attacks . . . 17
References . . . 17

6 Governance **19**
Executive Summary . . . 19
6.1 Legal Framework and Freedom of Expression . . . 19
6.2 Data Protection and Surveillance . . . 20

6.3 Telecommunications and Economic Governance 20
References 21

7 Strategic Synthesis & Roadmap **22**

8 Section 7: Strategic Synthesis & Roadmap **23**
8.1 1. Executive Summary: The "Big Picture" Diagnosis 23
8.2 2. SWOT Analysis: The Strategic Cheat Sheet 24
8.3 3. Strategic Roadmap: The Policy Agenda 25
8.4 4. Final Verdict 25

Chapter 1

Geopolitics

Executive Summary

Tunisia's geopolitical standing is currently defined by a strategic paradox: a political pivot toward Eastern powers contrasting with a deepening physical integration into Western digital infrastructure. While the country historically operated as a pro-Western neutral actor, economic fragility and political shifts have positioned it as a "swing country," increasingly engaging with Russia and China while distancing itself from traditional European Union (EU) and United States frameworks [Source 1]. Despite this diplomatic realignment, Tunisia's digital backbone remains heavily tethered to Europe through new high-capacity submarine cable projects like Medusa and energy interconnectors like ELMED [Source 4, Source 7].

The nation's "National Digital Strategy 2021-2025" explicitly prioritizes digital sovereignty and the protection of national cyberspace [Source 12]. However, intelligence indicates a critical vulnerability in this posture: a massive reliance on foreign third-party transit providers. Specifically, the network exhibits a severe chokepoint around Cloudflare (ASN 13335), upon which nearly 1,000 Autonomous Systems (ASNs) depend, creating a single point of failure that undermines claims of sovereign digital control [IYP-GRAPH]. Furthermore, the telecommunications sector remains dominated by state-owned monopolies and centralized incumbents, limiting the redundancy required for a resilient "digital fortress" [Source 6, IYP-GRAPH].

1.1 Geopolitical Alignment and Strategic Positioning

Tunisia's geopolitical trajectory is characterized by a departure from its traditional Western orientation. Driven by economic precariousness—including bankruptcy risks—and perceived insufficient engagement from the EU regarding migration and economic aid, Tunis is tilting toward Algeria and exploring deeper ties with Russia and China [Source 1, Source 3]. This shift enhances Russia's potential strategic posture in the Mediterranean, leveraging Tunisia's location as a choke point for maritime traffic and human migration routes [Source 1, Source 2].

Despite this political pivot, Tunisia remains enmeshed in Western digital governance frameworks.

The country is a participant in the EU-LAC Digital Alliance, a partnership model that implies adherence to EU-centric digital standards, facilitated by a strong cooperative history with Estonia regarding e-governance and institutional digitization [Source 9, Source 10]. This creates a complex dynamic where Tunisia's political rhetoric favors the East, while its technical and administrative standards continue to align with European norms to attract investment in digital services [Source 3].

1.2 Submarine Infrastructure and Regional Connectivity

Tunisia's physical connectivity strategy focuses on reinforcing its link to Southern Europe rather than serving as a gateway for landlocked African nations. Intelligence confirms that Tunisia does not currently serve as a digital transit hub for landlocked neighbors in the Sahel or Sub-Saharan Africa [Source (Q4)].

Instead, infrastructure development is concentrated on the Mediterranean interface: * **The Medusa Submarine Cable System:** This is a critical strategic asset connecting Tunisia to Southern Europe (Portugal, Spain, France, Italy, Greece, Cyprus) and North Africa (Morocco, Algeria, Egypt, Libya) [Source 4, Source 5]. The Tunisian landing station in Bizerte, managed by Orange Tunisia, will provide a capacity of 24 Tbps, reinforcing the country's status as a connectivity node for the Mediterranean basin [Source 14, Source 15]. * **Ownership Structure:** The infrastructure landscape is a hybrid of state monopoly and private foreign investment. The state-owned entity, Tunisie Telecom, holds a monopoly on international facilities [Source 6]. However, the Medusa project is promoted by the private entity AFR-IX TELECOM SA, indicating a shift toward allowing foreign private capital to develop critical cross-border links [Source 8]. * **Energy-Digital Nexus:** The ELMED project, primarily an energy interconnector with Italy managed by the state utility STEG, also includes fiber optic components, further cementing the physical tether to the Italian peninsula [Source 7].

1.3 Digital Sovereignty and Network Vulnerabilities

The Tunisian government has articulated a clear intent to achieve "Digital Sovereignty" through its National Digital Strategy 2021-2025, aiming to secure national cyberspace and foster a knowledge economy [Source 12, Source 13]. However, technical analysis of the country's internet architecture reveals significant dependencies that contradict these sovereignty goals.

Critical Chokepoints: Analysis of the country's routing architecture identifies **Cloudflare (ASN 13335)** as a massive external dependency. Approximately 956 ASNs within the Tunisian ecosystem depend on Cloudflare, giving this single US-based entity a "Chokepoint Score" that vastly exceeds local providers [IYP-GRAPH]. This indicates that a significant portion of Tunisia's traffic is subject to the operational stability and policy jurisdiction of a foreign Tier 1 operator.

Centralization of Domestic Control: The domestic network is highly centralized around

the incumbent operator, **TUNISIANA (ASN 37693)**, and the Tunisia BackBone (TN-BB-AS). Direct upstream transit providers for TUNISIANA are limited to TN-BB-AS and the Agence Tunisienne d'Internet (ATI-TN) [IYP-GRAPH]. Dependency scores (`d.hege`) indicate that smaller operators exhibit 100% dependency on these central nodes, creating a hierarchical topology where the incumbent retains absolute leverage over downstream traffic [IYP-GRAPH]. This centralization facilitates state control but increases vulnerability to targeted disruptions.

References

- [Source 1] Tunisia at the Crossroads: What Role for the United States in a Multipolar World (https://www.washingtoninstitute.org/policy-analysis/tunisia-crossroads-what-role-united-states-multipolar-world)
- [Source 2] Trying to understand the role north africa plays in global trade (https://www.reddit.com/r/geop
- [Source 3] Infectious Peace, Strategic Prosperity in North Africa: Why It Starts in Tunis (https://thegeopolitics.com/infectious-peace-strategic-prosperity-in-north-africa-why-it-starts-in-tunis/)
- [Source 4] Medusa submarine cable to connect to the Red Sea through Telecom Egypt (https://medusascs.com/news/medusa-submarine-cable-to-connect-to-the-red-sea-through-telecom-egypt/)
- [Source 5] Medusa and Libyan United International partner to land cable in Libya (https://medusascs.com/fr/news/medusa-and-libyan-united-international-partner-to-land-cable-in-libya/)
- [Source 6] Broadband Networks in the Middle East and North Africa - World Bank (https://www.worldbank.org/content/dam/Worldbank/document/MNA/Broadband_report/Broadband
- [Source 7] Elmed | Italy Tunisia submarine power line (https://elmedproject.com/)
- [Source 8] AFR-IX MEDUSA SUBMARINE CABLE SYSTEM (https://www.eib.org/en/projects/pipelin
- [Source 9] A Coded Revolution: How Tunisia And Estonia Digitized A Democratic Alliance (https://yris.yira.org/high-school-essay-contest/a-coded-revolution-how-tunisia-and-estonia-digitized-a-democratic-alliance/)
- [Source 10] EU-LAC Digital Alliance partners promote digital citizen engagement (https://www.eeas.europa.eu/eeas/eu-lac-digital-alliance-partners-promote-digital-citizen-engagement-central-america_en)
- [Source 11] EU-LAC Digital Alliance | EEAS (https://www.eeas.europa.eu/eeas/alianza-digital-ue-lac_en)
- [Source 12] Tunisia's National Digital Strategy 2021-2025 (https://dig.watch/resource/tunisias-national-digital-strategy-2021-2025)
- [Source 13] Tunisia attends 50th session of Arab Labour Conference in Iraq (https://www.social.gov.tn/en/tunisia-attends-50th-session-arab-labour-conference-iraq)
- [Source 14] Orange hosts the Medusa submarine cable at its infrastructure in Marseille (https://newsroom.orange.com/orange-hosts-the-medusa-submarine-cable-at-its-infrastructure-in-marseille-for-its-first-landing/)

- [Source 15] Orange Tunisia welcomes the new MEDUSA submarine cable (https://extensia.tech/orange-tunisia-welcomes-the-new-medusa-submarine-cable/)
- [IYP-GRAPH] Internal Knowledge Graph (Technical Network Analysis)

Chapter 2

Infrastructure

Executive Summary

Tunisia's telecommunications infrastructure is currently in a transitional phase, characterized by significant advancements in mobile network capabilities alongside persistent challenges in fixed broadband and legacy systems. The recent commercial launch of 5G services, utilizing a spectrum mix of 700 MHz and 3500 MHz, has resulted in substantial performance gains, with median download speeds exceeding 300 Mbps [Source 1][Source 2]. However, the fixed broadband sector remains constrained by infrastructure gaps, particularly in rural areas where service quality is fragile and falls below international benchmarks [Source 3].

Internationally, Tunisia is strengthening its connectivity through the Medusa Submarine Cable System, which connects the country to France and Morocco, mitigating historical bottlenecks caused by incumbent monopolies on landing stations [Source 4][Source 5]. Internally, the network topology is heavily concentrated; analysis of the country's 11 Autonomous System Numbers (ASNs) reveals that CloudflareNet and Topnet serve as critical dependency nodes, indicating potential chokepoints in the digital supply chain [Source 6][Source 7]. While the country has engaged in Internet Exchange Point (IXP) development, the retention of legacy IT systems continues to hinder the widespread adoption of cloud-based services and AI technologies [Source 3][Source 8].

2.1 Mobile and Fixed Network Architecture

Mobile Network Evolution Tunisia has actively moved toward the deployment of next-generation mobile networks. The country launched commercial 5G services in February, utilizing a spectrum allocation strategy that combines the 700 MHz band for coverage and the 3500 MHz band for capacity. This deployment has delivered immediate operational improvements, with median mobile download speeds reportedly jumping to over 300 Mbps [Source 1]. Despite these gains, specific data regarding 5G population coverage percentages remains unavailable, and detailed roadmaps for future spectrum auctions have not been publicly released beyond the initial

allocation [Source 2].

Fixed Broadband and Digital Divide In contrast to the mobile sector, fixed broadband infrastructure faces significant structural hurdles. While IPv6 adoption is progressing—with Tunisie Telecom and Tunisiana deploying the protocol and competitors like Topnet and Orange Tunisia planning implementation—overall fixed broadband quality remains uneven [Source 9]. Strategic analysis indicates a sharp digital divide; major urban centers benefit from superior bandwidth and 4G coverage, whereas rural and remote regions suffer from "white spots" and fragile connectivity [Source 3]. The fixed market is historically dominated by Tunisie Telecom, and the lack of competitive pressure has slowed the replacement of legacy copper networks with Fiber to the Home (FTTH), for which no definitive penetration rates are currently available [Source 9][Source 10].

2.2 International Connectivity and Submarine Cables

Tunisia's international bandwidth reliability is heavily dependent on submarine cable infrastructure. A critical development is the Medusa Submarine Cable System, which has completed its final splice physically connecting Tunisia with France and Morocco. This system is designed to diversify routes and increase capacity across the Mediterranean [Source 4].

Historically, the incumbent operator, Tunisie Telecom, has maintained a monopoly on international landing stations, a factor that the World Bank identifies as a barrier to competition and open access for alternative infrastructure providers [Source 5]. The operationalization of the Medusa system represents a strategic shift, potentially reducing reliance on legacy routes and improving the resilience of Tunisia's gateway to the global internet.

2.3 Network Topology and Critical Dependencies

ASN Distribution and IP Concentration Tunisia's internal internet structure is comprised of 11 Autonomous System Numbers (ASNs). Network analysis reveals a high concentration of IP prefixes within specific entities. CloudflareNet holds the largest share with 10,880 prefixes (4,799 IPv4 and 6,081 IPv6), followed by Tunisiana with 3,071 prefixes. This unusual concentration suggests a heavy reliance on external Content Delivery Networks (CDNs) and security infrastructure for traffic management within the national border [Source 6].

Chokepoints and Market Reach Graph analysis identifies critical chokepoints within the national backbone. TOPNET and CLOUDFLARENET each maintain seven incoming dependency relationships (`DEPENDS_ON`), making them central nodes where failure could cascade across the network. ATI-ISP and Tunisie-Telecom follow with five and four dependencies, respectively [Source 7]. In terms of population reach, Tunisiana leads with access to approximately 30.98% of the population, followed by TOPNET (25.74%) and Orange (20.78%), highlighting the dominance of these three entities in the consumer market [Source 11].

2.4 Internet Exchange Points (IXPs) and Peering

The domestic traffic exchange ecosystem is anchored by TunIXP. Current intelligence identifies six active ASNs registered as members of TunIXP: ATI-TN (Agence Tunisienne d'Internet), AFRINIC-Anycast nodes, TN-BB-AS (Tunisia BackBone), and PCH-AS [Source 11].

While specific details on the physical geographical distribution of these exchange points are limited, historical data indicates that Tunisia participated in capacity-building workshops for "AXIS-New IXP" development between 2014 and 2016 [Source 12]. The current operational status suggests a centralized peering model managed largely through state-affiliated entities like ATI, rather than a diverse ecosystem of commercial carrier-neutral exchanges.

2.5 Data Center and Cloud Infrastructure

Tunisia's hosting infrastructure lacks a significant presence from global hyperscale providers. Major international operators such as NTT DATA and Equinix do not list Tunisia among their data center locations in the EMEA region [Source 13][Source 14]. Consequently, the domestic cloud market is underdeveloped.

The persistence of legacy IT systems within the public and private sectors is a primary inhibitor to digital transformation. Unlike markets that have migrated to scalable cloud architectures, Tunisian entities often maintain older, on-premise systems, limiting the potential for deploying advanced AI and cloud-based services that require robust, elastic infrastructure [Source 3][Source 8].

References

- [Source 1] 5G Helped Egypt and Tunisia Uplift Mobile Performance to New… (https://www.ookla.com/articles/5g-north-africa-2025)
- [Source 2] 5G in Africa 2023: market status, trends and outlook - GSMA (https://event-assets.gsma.com/pdf/5G-in-Africa-2023.pdf)
- [Source 3] Digital Transformation in Tunisia: Under Which Conditions Could the… (https://shs.hal.science/halshs-03506136v1/document)
- [Source 4] Medusa Submarine Cable System - LinkedIn (https://www.linkedin.com/company/medusa-submarine-cable-system/)
- [Source 5] Broadband Networks in the Middle East and North Africa - World Bank (https://www.worldbank.org/content/dam/Worldbank/document/MNA/Broadband_report/Broadband
- [Source 6] Internal Graph (ASN Prefix Distribution)
- [Source 7] Internal Graph (ASN Dependencies)
- [Source 8] Cloud Services Advance Digital Transformation for Governments (https://www.worldbank.org/
services-advance-digital-transformation-for-governments)
- [Source 9] IPv6 adoption is hitting record numbers around the world … - Reddit (https://www.reddit.com/r/ipv6/comments/1aqi6vy/ipv6_adoption_is_hitting_record_numbers_arou

- [Source 10] Tunisia Infrastructure Diagnostic - Open Knowledge Repository (https://openknowledge.world 2e97-5bc3-bfa5-5114181ddcd5/content)
- [Source 11] Internal Graph (IXP Membership and Reach)
- [Source 12] Interconnection and Traffic exchange towards 80% locally accessed … (https://www.internetsociety.org/wp-content/uploads/2017/08/Brochure_-_Interconnection_and_Traff
- [Source 13] Global Data Centers | NTT DATA (https://services.global.ntt/en-us/services-and-products/global-data-centers)
- [Source 14] Europe, Middle East and Africa Data Center Colocation … - Equinix (https://www.equinix.com/data-centers/europe-colocation)

Chapter 3

Market

Executive Summary

The Tunisian telecommunications market operates as a rigid oligopoly characterized by high concentration and significant state influence over critical infrastructure. The sector is dominated by three primary operators—Ooredoo Tunisia, Orange Tunisie, and the state-owned enterprise (SOE) Tunisie Télécom—which collectively control the mobile and fixed-line segments. While Ooredoo has emerged as the leader in mobile subscriber market share, holding approximately 47% of the market, Tunisie Télécom retains a de facto monopoly on fixed-line communications and international submarine cable landing stations [Source 1][Source 2].

Despite the competitive presence of three major players, the market lacks a "disruptor" entity capable of driving down costs or introducing radical service tier changes [Source 3]. Consequently, mobile data pricing in Tunisia remains high relative to the region, averaging USD 1.78 per gigabyte (GB), which is more than double the North African average of USD 0.86 [Source 4][Source 5]. Network performance indicators reveal a disparity between mobile and fixed services; median mobile download speeds (21.64 Mbps) significantly outperform fixed broadband (11.72 Mbps), reflecting underinvestment and bottlenecks in fixed infrastructure [Source 6][Source 7]. Regulatory barriers and the lack of infrastructure sharing continue to impede market efficiency and broadband uptake [Source 8].

3.1 Market Structure and Competitive Landscape

The mobile sector is defined by a three-player structure with shifting dominance. Recent data indicates that Ooredoo has secured the leading position with a 47% subscriber market share, followed by Orange at 29.9% and Tunisie Télécom at 23.1% [Source 1]. This represents a notable shift from 2022, where Tunisie Télécom held a plurality of the market (39.7%), suggesting aggressive customer acquisition or retention strategies by Ooredoo in the interim period [Source 2]. The market impact of Mobile Virtual Network Operators (MVNOs) remains negligible, with Lycamobile holding an insignificant share [Source 2].

The broader telecommunications environment exhibits signs of a duopoly or oligopoly rather than a fully liberalized market. State-owned enterprises (SOEs) create high barriers to entry. Specifically, Tunisie Télécom's control over the fixed-line network and international connectivity gateways creates a bottleneck that restricts competition and sustains high service costs [Source 9]. There is no evidence of recent mergers and acquisitions (M&A) activity or the entry of disruptive competitors that could alter this entrenched structure [Source 3][Source 10].

3.2 Pricing and Affordability Analysis

The cost of mobile data in Tunisia presents a barrier to broader digital inclusion when compared to regional peers. The average price for 1GB of mobile data is USD 1.78 [Source 4]. While this figure is lower than the Western European average of USD 2.08, it is significantly higher than the North African average of USD 0.86, indicating that Tunisian consumers pay a premium relative to their immediate geographic neighbors [Source 5].

High pricing is attributed to structural inefficiencies. The World Bank identifies the dominance of Tunisie Télécom in the fixed broadband market and restrictions on new entrants as primary drivers of high costs [Source 8]. Furthermore, the lack of mandatory infrastructure sharing among operators prevents capital expenditure optimization, keeping consumer prices elevated [Source 8]. While specific data regarding the cost of a basic data package relative to the minimum wage is inconclusive, international bodies note that high data costs generally impede broadband uptake in middle-income economies like Tunisia [Source 11].

3.3 Network Infrastructure and Performance

Tunisia's network performance metrics highlight a divergence between mobile and fixed connectivity. The median mobile download speed stands at 21.64 Mbps, with an upload speed of 8.96 Mbps [Source 6]. In contrast, fixed broadband lags significantly, offering a median download speed of only 11.72 Mbps [Source 7]. This discrepancy underscores the reliance of the population on mobile networks for high-speed internet access, likely due to the limitations of the fixed-line infrastructure controlled by the state incumbent.

Information regarding specific Quality of Service (QoS) metrics, such as call drop rates or latency, is not publicly detailed in current intelligence, preventing a granular comparison of operator performance [Source 6][Source 12]. However, the infrastructure bottlenecks identified—specifically regarding international submarine cables—suggest that latency and consistency may be challenged during peak usage periods [Source 9].

References

- [Source 1] Mobile connectivity solutions in Tunisia 2025 - GoMoWorld (https://www.gomoworld.com/en/b
esim-and-sim-card-tunisia)

- [Source 2] Tunisia - Telecommunications Equipment & Services (https://www.trade.gov/country-commercial-guides/tunisia-telecommunications-equipment-services)
- [Source 3] FOREIGN TRADE BARRIERS - USTR (https://ustr.gov/sites/default/files/files/Press/Repo
- [Source 4] The Most Expensive Data Prices in Africa (https://www.connectingafrica.com/digital-inclusion/the-most-expensive-data-prices-in-africa)
- [Source 5] The Cost of 1GB Of Mobile Data in 237 Countries - Broadband Deals (https://bestbroadbanddeals.co.uk/mobiles/worldwide-data-pricing/)
- [Source 6] Tunisia's Mobile and Broadband Internet Speeds - Speedtest Global Index (https://www.speedtest.net/global-index/tunisia)
- [Source 7] Fiber Brings Faster Fixed Broadband to North Africa with … - Ookla (https://www.ookla.com/articles/fixed-speeds-north-africa-2024)
- [Source 8] Tunisia Infrastructure Diagnostic - Open Knowledge Repository (https://openknowledge.worldb 2e97-5bc3-bfa5-5114181ddcd5/content)
- [Source 9] The Unfinished Revolution: Bringing Opportunity, Good Jobs and Greater Wealth to All Tunisians (https://www.worldbank.org/content/dam/Worldbank/document/MNA/tunisia
- [Source 10] M&A trends in tech, media, and telecom - KPMG International (https://kpmg.com/us/en/articles/mergers-acquisitions-trends-tech-media-telecom.html)
- [Source 11] The affordability of ICT services - ITU (https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICT_PRICES.01-2025-PDF-E.pdf)
- [Source 12] End to End QoS Metrics Modeling Based on Multi-application … (https://pubs.sciepub.com/jcn/4/1/1/index.html)

Chapter 4

Localization

Executive Summary

Tunisia's approach to data localization and digital sovereignty is currently defined by regulatory enforcement rather than a publicly articulated industrial strategy for sovereign infrastructure. Unlike Gulf Cooperation Council (GCC) states, which have aggressively pursued comprehensive digital sovereignty frameworks, Tunisia lacks a definitive, open-source strategy for a "National Cloud" or specific incentives for localizing cloud services [Source 1 (Q4)]. However, the Tunisian Data Protection Authority has demonstrated a willingness to enforce de facto localization through existing privacy laws, evidenced by legal proceedings against hosting providers for unauthorized cross-border data transfers [Source 1 (Q9)]. The market remains opaque regarding the specific share of hyperscale providers versus local entities, indicating a significant intelligence gap in the commercial landscape of national data hosting [Source 1 (Q3)].

Regulatory Framework and Enforcement

The primary mechanism for data localization in Tunisia appears to be the enforcement of data protection mandates rather than explicit data residency legislation. Regulatory bodies have taken punitive measures to ensure transparency regarding data storage locations. Notably, the Tunisian Data Protection Authority instituted proceedings against OVH Tunisie. The charges focused on the provider's failure to disclose data storage locations, failure to obtain necessary user consent, and the execution of data transfers abroad without authorization [Source 1 (Q9)].

This enforcement action establishes a critical precedent: while specific laws mandating that all data remain within Tunisian borders may not be explicitly codified in a single "Localization Act," the regulatory interpretation of data privacy effectively restricts the free flow of sensitive data to foreign jurisdictions without strict compliance. This creates a compliance-driven localization environment where entities may default to local hosting to avoid regulatory scrutiny regarding cross-border transfer protocols.

Digital Sovereignty and Infrastructure Maturity

Tunisia occupies a challenging position within the broader Middle East and North Africa (MENA) digital landscape. Regional analysis indicates that North African countries, including Tunisia, lag significantly behind Gulf countries regarding digital infrastructure capabilities and regional coordination [Source 1 (Q4)]. The nation faces systemic challenges related to technological dependencies on foreign firms, a common issue for developing economies striving for digital sovereignty [Source 1 (Q12)].

There is currently no definitive open-source intelligence detailing the market share breakdown between global hyperscale providers (AWS, Azure, Google Cloud) and local Tunisian hosting companies [Source 1 (Q3)]. Furthermore, no official government policy has been identified that explicitly promotes the adoption of local cloud infrastructure as a means to enhance digital sovereignty [Source 1 (Q4)]. This suggests that while the *legal* risk of foreign hosting is being policed, the *technical* alternative—a robust, state-supported domestic cloud ecosystem—may not yet be fully realized or incentivized by current policy frameworks.

Public Sector Security and E-Government

The security and hosting of public sector digital services remain a critical area of development. The UN E-Government Survey 2024 identifies the bolstering of cybersecurity and the establishment of robust legal frameworks for data privacy as essential components for e-government advancement [Source 1 (Q6)]. While specific metrics on the percentage of national data hosted locally versus internationally are unavailable [Source 1 (Q2)], the emphasis on legal frameworks in international assessments corroborates the domestic focus on regulatory enforcement seen in the private sector.

References

- [Source 1 (Q3)] Public cloud revenue: Spending boom for AWS, Azure and Google (https://www.techmonitor.ai/cloud/public-cloud-revenue-aws-azure-google-cloud/)
- [Source 1 (Q4)] DIGITAL SOVEREIGNTY IN THE MENA REGION - EuroMeSCo (https://www.euromesco.net/wp-content/uploads/2024/10/Policy-Study36.pdf)
- [Source 1 (Q9)] Which Way for Data Localisation in Africa? Brief - CIPESA (https://cipesa.org/download/briefs/Which_Way_for_Data_Localisation_in_Africa____Brief.pdf)
- [Source 1 (Q6)] E-Government Survey 2024 (https://desapublications.un.org/sites/default/files/publicatio 09/%28Web%20version%29%20E-Government%20Survey%202024%201392024.pdf)
- [Source 1 (Q12)] Global approaches to digital sovereignty: Competing definitions and contrasting policy - ECDPM (https://ecdpm.org/application/files/7816/8485/0476/Global-approaches-digital-sovereignty-competing-definitions-contrasting-policy-ECDPM-Discussion-Paper-344-2023.pdf)
- [Source 1 (Q2)] FOREIGN TRADE BARRIERS - USTR (https://ustr.gov/sites/default/files/files/Press/

Chapter 5

Security

Executive Summary

Tunisia exhibits a mature cybersecurity posture relative to its regional peers, characterized by strong national preparedness rankings and robust routing security protocols. The nation ranks 38th on the National Cyber Security Index (NCSI), outperforming neighboring states in the Maghreb and North Africa [Source 3]. A key strength in Tunisia's defensive architecture is its adoption of Resource Public Key Infrastructure (RPKI), with over 61% of IP prefixes validating Route Origin Authorizations (ROAs), significantly mitigating the risk of accidental route leaks [IYP-GRAPH].

However, the Tunisian digital landscape faces distinct threats, primarily from high-intensity Distributed Denial of Service (DDoS) attacks targeting critical telecommunications infrastructure. Recent intelligence indicates that wired telecommunications carriers face prolonged and high-volume attacks, with peak intensities exceeding 750 Gbps [Source 1]. Furthermore, network topology analysis reveals a high degree of centralization, with international service providers acting as significant chokepoints for inbound traffic, potentially creating single points of failure [IYP-GRAPH]. While basic routing security is established, data regarding advanced protocol adoption such as DNSSEC and MANRS remains limited or unavailable [IYP-GRAPH].

5.1 National Cybersecurity Posture and Governance

Tunisia maintains a competitive standing in global and regional cybersecurity indices, reflecting a concerted effort to establish legal frameworks and technical capacity. On the National Cyber Security Index (NCSI), Tunisia holds the 38th position globally with a score of 79.17 [Source 3]. This ranking places it favorably against regional counterparts, scoring slightly higher than Morocco (39th) and significantly outperforming Egypt (58th) and Algeria (96th) [Source 1].

The country's performance is underpinned by factors critical to the ITU Global Cybersecurity Index (GCI), including the implementation of technical measures, organizational structures, and capacity development programs [Source 2]. Despite these strengths, the specific adoption rates

for advanced security protocols such as DNSSEC remain unclear, with validation status for DNS queries originating from Tunisia consistently reported as unknown [IYP-GRAPH].

5.2 Network Infrastructure and Routing Security

The integrity of Tunisia's routing infrastructure is relatively high. Intelligence confirms that 61.32% of Tunisian IP prefixes have validated RPKI Route Origin Authorizations (ROAs) configured, a critical defense against BGP hijacking [IYP-GRAPH]. Consistent with this preventative posture, there have been no known BGP hijacking incidents or significant route leaks demonstrably impacting Tunisian internet connectivity over the past two years [IYP-GRAPH].

However, the topological structure of the Tunisian internet exhibits signs of centralization. Dependency analysis identifies CLOUDFLARENET as a major "chokepoint" for inbound traffic, with 956 Autonomous System Numbers (ASNs) depending on it [IYP-GRAPH]. Domestic infrastructure also shows centralization, with TN-BB-AS (Tunisia BackBone AS) and TUNISIANA serving as key nodes with 18 and 14 dependencies respectively [IYP-GRAPH]. Technical data regarding the participation of Tunisian ASNs in the Mutually Agreed Norms for Routing Security (MANRS) is currently unavailable [IYP-GRAPH].

5.3 Threat Landscape: DDoS and Volumetric Attacks

The primary operational threat to Tunisian networks is volumetric DDoS activity, mirroring a broader regional trend where attacks in the MENA region surged by 216% in 2024 [Source 4]. Between January and June 2025, the telecommunications sector was the primary target of these hostilities.

Wired Telecommunications Carriers sustained the most severe assaults, with an average attack duration of 500 minutes and a maximum attack intensity of 756.61 Gbps [Source 1]. Wireless Telecommunications Carriers faced shorter, high-intensity bursts, averaging 15 minutes in duration with peak volumes of 120.55 Gbps [Source 1]. The hospitality sector (Hotels and Motels) was the third most targeted industry, experiencing attacks averaging 12 minutes with peaks of 57.71 Gbps [Source 1]. While global reports indicate a rise in malware and botnet activity, specific infection rates for Tunisia are not currently available in open-source intelligence [Source 5].

References

- [Source 1] Tunisia - Latest Cyber Threat Intelligence Report (https://www.netscout.com/threatreport/cou
- [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] NCSI :: Ranking - National Cyber Security Index (https://ncsi.ega.ee/ncsi-index/?order=rank)

- [Source 4] DDoS Attacks in MENA: 2024 Report - StormWall (https://stormwall.network/resources/blog/
ddos-attacks-mena)
- [Source 5] Annual Threat Assessment of the U.S. Intelligence Community (https://www.dni.gov/files/ODN
2023-Unclassified-Report.pdf)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 6

Governance

Executive Summary

Tunisia's governance landscape, particularly regarding the digital domain and civil liberties, has undergone a significant shift toward authoritarianism and state control, diverging sharply from the democratic aspirations of the post-2011 revolution era. Recent intelligence indicates a transition toward a governance model prioritizing state surveillance and the suppression of dissent, akin to the "Beijing Model," rather than a rights-based regulatory framework [Source 12.1][Source 12.2].

The consolidation of executive power since July 2021 has resulted in the erosion of judicial independence and the weaponization of the legal system against political opponents [Source 3.4]. The promulgation of **Decree-Law 54** in September 2022 represents a critical inflection point, criminalizing "false information" and effectively curbing freedom of expression online [Source 9.2]. While the **Startup Act of 2018** remains a positive legislative framework for economic innovation [Source 11.2], it stands in contrast to a broader environment characterized by weak data protection enforcement, opaque surveillance initiatives, and the use of vague national security provisions to justify internet restrictions [Source 3.2][Source 5.1].

6.1 Legal Framework and Freedom of Expression

The current legal environment in Tunisia is defined by the use of restrictive legislation to dismantle online activist networks and suppress political opposition. Authorities increasingly rely on vague provisions within the Penal Code and anti-terrorism laws to target critics, lawyers, and journalists [Source 3.2][Source 3.4].

Decree-Law 54: Enacted on September 13, 2022, this decree is the primary instrument for prosecuting online speech. Ostensibly designed to fight cybercrime, it imposes severe penalties—including prison sentences of up to 10 years—for spreading "false information and rumors online" [Source 12.2]. This law has been utilized to prosecute individuals in high-profile instances such as the "Conspiracy Case" and the "Instalingo Case," undermining constitutional guarantees of

freedom of opinion [Source 9.1][Source 9.2].

Censorship and Internet Controls: While specific technical details on recent internet shutdown mechanisms are opaque, the government retains the ability to restrict access based on "security reasons" and the maintenance of "public order" [Source 8.3]. Historical data indicates a capacity for pervasive censorship, including the blocking of platforms and the prohibition of VoIP services, a capability that remains a latent threat given the current security-centric governance posture [Source 4.1].

6.2 Data Protection and Surveillance

Tunisia's data protection regime is currently insufficient to safeguard citizens against unwarranted government intrusion, characterized by obsolete legislation and a lack of transparency in state digitization projects.

Legislative Gaps: The primary legislation, the **Data Protection Law of 2004**, is considered obsolete and ineffectively enforced [Source 5.1]. Although the law establishes the *Institut National de la Protection des Données Personnelles* (INPDP) and mandates authorization for cross-border data transfers (Article 52) [Source 6.1], Tunisia has not received an EU adequacy decision, nor has it ratified the Budapest Convention on Cybercrime [Source 2.1][Source 6.2].

Surveillance Infrastructure: Significant concerns exist regarding the **Biometric ID** and **Mobile ID (e-houwiya)** programs. These initiatives have been developed with minimal civil society input or transparency regarding data management and security [Source 5.1]. Intelligence suggests that the lack of robust safeguards, combined with a history of cyberattacks, leaves the biometric data of citizens vulnerable to misuse and state surveillance [Source 5.1].

6.3 Telecommunications and Economic Governance

The governance of the telecommunications sector reflects a hybrid model of market competition and lingering state influence.

Market Structure and Licensing: The telecommunications sector has been opened to private competition and foreign investment, with Tunisia committing to WTO telecom service sector standards [Source 7.2]. However, the post-2011 nationalization of assets belonging to the former regime has left the state with significant shareholdings in major operators (e.g., Ooredoo and Orange Tunisie), creating potential conflicts of interest in regulatory oversight [Source 7.2].

Regulatory Independence: Information regarding the independence of the Tunisian National Telecommunications Authority (INT), specifically concerning leadership appointments and budgetary autonomy, remains opaque in current reporting [Source 1.1].

Digital Economy: Conversely, the **Startup Act (2018)** represents a successful governance initiative aimed at fostering entrepreneurship. It simplifies business transactions and incentivizes

investment, serving as a rare example of policy innovation designed to spur economic demand rather than control [Source 11.2].

References

- [Source 1.1] Enhancing the Rule of Law and guaranteeing human rights in the … (https://www.icj.org/wp-content/uploads/2013/02/TUNISIA-CONSTITUTION-REPORT-FINAL.pdf)
- [Source 2.1] Cybercrime legislation - https: //rm. coe. int (https://rm.coe.int/tunisia-en/1680aef827)
- [Source 3.2] Tunisia authorities criticized over crackdown on peaceful protesters … (https://www.jurist.org/news/2025/06/tunisian-authorities-criticized-over-crackdown-on-peaceful-protesters-and-opposition-amid-deepening-crisis/)
- [Source 3.4] HRW: Tunisia government using arbitrary detention to suppress … (https://www.jurist.org/news/2025/04/hrw-tunisia-government-using-arbitrary-detention-to-suppress-dissent/)
- [Source 4.1] TUNISIA - Freedom House (https://www.freedomhouse.org/sites/default/files/inline_images
- [Source 5.1] Tunisia's digitization programs threaten the privacy of millions - SMEX (https://smex.org/tunisias-digitization-programs-threaten-the-privacy-of-millions/)
- [Source 6.1] Application of Tunisian Legislation on Personal Data Protection (https://bkassocies.tn/en/practical-guide-application-of-tunisian-legislation-on-personal-data-protection/)
- [Source 6.2] Data Protection Laws in Northern Africa - Konrad-Adenauer-Stiftung (https://www.kas.de/documents/265308/22468903/230406_DataProtectionLawsNorthernAfrica_KAS_
- [Source 7.2] Tunisia - Telecommunications Equipment & Services (https://www.trade.gov/country-commercial-guides/tunisia-telecommunications-equipment-services)
- [Source 8.3] Joint letter on internet shutdown in Uganda (https://www.apc.org/en/pubs/joint-letter-internet-shutdown-uganda)
- [Source 9.1] "All Conspirators": How Tunisia Uses Arbitrary Detention to Crush … (https://www.hrw.org/report/2025/04/16/all-conspirators/how-tunisia-uses-arbitrary-detention-crush-dissent)
- [Source 9.2] Tunisia: Silencing Free Voices A briefing paper on the enforcement … (https://www.icj.org/wp-content/uploads/2023/07/Tunisia-Silencing-Free-Voices-_compressed-1.pdf)
- [Source 11.2] Startup Acts are the next form of policy innovation in Africa (https://www.atlanticcouncil.org
acts-are-the-next-form-of-policy-innovation-in-africa/)
- [Source 12.1] Using AI as a weapon of repression and its impact on human rights (https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450_EN.p
- [Source 12.2] Tunisia Country Report 2024 - BTI Transformation Index (https://bti-project.org/en/reports/country-report/TUN)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 7

Strategic Synthesis & Roadmap

Chapter 8

Section 7: Strategic Synthesis & Roadmap

To: The President / Prime Minister of the Republic of Tunisia **From:** Office of the Chief Strategy Officer **Date:** October 26, 2025 **Subject:** STATE OF THE NETWORK – The "Sovereignty Paradox"

8.1 1. Executive Summary: The "Big Picture" Diagnosis

The Narrative: The Digital Carthage Strategy Tunisia stands at a defining historical juncture. We have successfully deployed 5G and secured our position as a Mediterranean landing hub via the Medusa cable. However, our digital posture is dangerously misaligned with our geopolitical trajectory. While we pivot politically toward the "Global East" (deepening ties with Russia, China, and Algeria), our digital nervous system remains almost entirely dependent on Western infrastructure and US-based corporate jurisdiction.

The Paradox: "Political Autonomy vs. Digital Dependency" We claim "Digital Sovereignty" as a national priority, yet our network topology reveals a critical fragility: **The Cloudflare Chokepoint.** While we project strength through authoritarian governance and anti-Western rhetoric, nearly 1,000 of our autonomous networks depend on a single US company (Cloudflare) for security and routing. If geopolitical tensions rise, Tunisia does not need to be invaded to be neutralized; we can be "switched off" by a foreign corporate policy change or a targeted sanction. We are building a fortress with a back door we do not hold the key to.

8.2 2. SWOT Analysis: The Strategic Cheat Sheet

8.2.1 Strengths (Leverage These)

- **Geographic Primacy:** The Bizerte landing station (Medusa) and ELMED energy link position us as the ideal data corridor between Europe and Africa.
- **Routing Hygiene:** We rank highly in routing security (RPKI adoption >61%), meaning our network is resistant to hijacking—a rare asset in the region.
- **Mobile Agility:** The rapid 5G rollout (300+ Mbps) proves our mobile operators can execute modernization quickly when permitted.
- **Innovation Framework:** The "Startup Act" remains a best-in-class policy that attracts talent despite broader economic headwinds.

8.2.2 Weaknesses (Fix These)

- **The "Cloudflare Risk":** Extreme centralization of inbound traffic through one US provider creates a single point of national failure.
- **Fixed-Line Stagnation:** The rural "white spots" and low fixed speeds (11 Mbps) are caused by the state monopoly (Tunisie Télécom) refusing to share infrastructure.
- **Data Hosting Void:** We lack local hyperscale data centers (AWS/Azure/Local equivalents), forcing our data to reside in Europe, subject to EU law, not ours.
- **High Consumer Costs:** Data prices ($1.78/GB) are double the North African average, stifling the digital economy.

8.2.3 Opportunities (Capture These)

- **"Green Data" Hub:** Leverage the ELMED energy interconnector to build green data centers. Sell "low-carbon computing" to Europe.
- **The "Digital Switzerland":** Position Tunisia as a neutral data haven for the Maghreb, offering strict privacy laws (enforced) and sovereign hosting that is neither fully Western nor Eastern aligned.
- **Nearshoring 2.0:** Move beyond call centers to high-value AI and cloud engineering, leveraging our time zone alignment with the EU.

8.2.4 Threats (Mitigate These)

- **DDoS Warfare:** Our telecom carriers are currently facing high-intensity attacks (>750 Gbps). This is economic sabotage targeting our connectivity.
- **Sanctions Vulnerability:** If we pivot too hard toward Russia, Western tech providers (Microsoft, Cloudflare) could restrict access, crippling our banking and government sectors.
- **Brain Drain:** Authoritarian drift and Decree 54 are scaring away the very engineers needed to build our sovereign cloud.

8.3 3. Strategic Roadmap: The Policy Agenda

8.3.1 Phase 1: Immediate Defense (Months 1-6) – "Secure the Perimeter"

- **Action 1: The "Multi-Vendor" Mandate.** Issue a decree requiring all Critical Infrastructure (Gov, Banking, Energy) to diversify CDN and Security providers. Reliance on Cloudflare alone must end. We must integrate a secondary, non-US alternative (e.g., local or neutral-state provider) to ensure redundancy.
- **Action 2: Anti-DDoS Shield.** Establish a National Cyber-Defense Center specifically for the Telecom sector. The state must subsidize DDoS mitigation hardware for Ooredoo, Orange, and TT to stop the current wave of attacks from degrading national productivity.
- **Action 3: Price Cap on Wholesale Data.** Direct the regulator (INT) to force a reduction in wholesale bandwidth rates charged by Tunisie Télécom. We must lower the consumer price of data to under $1.00/GB to match regional peers.

8.3.2 Phase 2: Structural Reform (Months 6-18) – "Break the Bottlenecks"

- **Action 1: End the Fixed-Line Monopoly.** Open the "last mile" infrastructure to competition. Allow private operators (Orange/Ooredoo) to lay their own fiber in rural areas where the state incumbent has failed to invest.
- **Action 2: The "Sovereign Cloud" Initiative.** Incentivize the construction of a Tier IV Data Center on Tunisian soil. Offer tax holidays and energy subsidies (via STEG) to a consortium that builds local hosting capacity. **Goal:** Keep Tunisian government data in Tunisia.
- **Action 3: Reform Decree 54.** Amend the "fake news" law to protect technical researchers and ethical hackers. Currently, security professionals are afraid to report vulnerabilities for fear of arrest. We need them on our side.

8.3.3 Phase 3: Long-Term Vision (Years 2-5) – "The Digital Gateway"

- **Action 1: The Trans-Sahara Link.** Stop looking only at Europe. Invest in terrestrial fiber links South to Algeria and Libya. Become the transit hub for landlocked African nations, selling them the bandwidth we import via Medusa.
- **Action 2: AI Sovereignty.** Utilize our local data centers to train "National AI" models on Tunisian datasets (dialect, law, culture), reducing reliance on Silicon Valley AI that does not understand our context.

8.4 4. Final Verdict

8.4.1 Investability Score: MEDIUM

- **Why:** Tunisia offers excellent physical connectivity (cables) and human capital (engineers). However, the **Governance Risk** (arbitrary detention, opaque laws) and **Market**

Rigidity (state monopolies) deter the massive foreign direct investment (FDI) needed for hyperscale growth. Investors love the location but fear the law.

8.4.2 Maturity Score: DEVELOPING (High Potential)

- **Why:** We are a "two-speed" nation. Our mobile network and routing security are **Mature** (First World standards). Our fixed infrastructure, cloud ecosystem, and market competition are **Emerging** (Third World standards). We have the engine of a Ferrari (5G/Medusa) inside the chassis of a bus (Copper lines/Monopolies).

Chief Strategy Officer's Note: *Mr. President, we cannot preach sovereignty while our digital existence depends on a server in Virginia. The path to true power lies in building our own cloud, breaking our own monopolies, and securing our own perimeter. Let us turn the "Paradox" into a "Fortress."*