STRATEGIC COUNTRY REPORT: TURKEY

Automated Strategic Analyst (v2.2 Parallel)

12 February 2026

Contents

Chapter 1

Geopolitics

Executive Summary

Turkey's geopolitical strategy in the digital domain is defined by an aggressive pursuit of "digital sovereignty," viewing cyberspace not merely as a technical utility but as a critical frontier for national security and political projection. The state characterizes the current global environment as a "techno-polar" order, necessitating robust national control over digital infrastructure and data flows to safeguard societal values and state interests [Source 1] [Source 3]. While Turkey actively positions itself as a physical and digital bridge between Europe and Asia—evidenced by its participation in the European Union's Black Sea connectivity agenda and alignment with China's Belt and Road Initiative (BRI)—its internal policy emphasizes resilience against foreign influence [Source 1] [Source 3]. The incumbent telecommunications operator, ASN 15924, maintains a diverse set of transit relationships, including connections with both Western entities and Chinese providers like Huawei Cloud, reflecting a multi-vector foreign policy approach [Internal Graph]. However, regional political tensions, particularly with Armenia, continue to dictate physical connectivity routes, limiting direct fiber optic integration with certain landlocked neighbors [Source 3].

1.1 Strategic Doctrine: Digital Sovereignty and the Techno-Polar Order

Turkey's current geopolitical stance regarding international internet connectivity is driven by the recognition that technological power is increasingly central to the global order. The state views cybersecurity as a vital component of foreign policy and national sovereignty, moving beyond technical defense to address political and societal security [Source 1]. This doctrine manifests in a strong emphasis on asserting national control over digital infrastructure and data, with the government actively developing policies to build resilience against transnational cyber threats [Source 3].

The Turkish administration engages in dialogues with the European Union to navigate emerging

technologies, exploring the digitalization of customs and borders as a mechanism to strengthen bilateral relations [Source 2]. However, this engagement is balanced by a strict adherence to national priorities, where digital sovereignty is leveraged to secure the domestic space while utilizing technological advancements for economic leverage [Source 3].

1.2 Network Topology and Transit Dynamics

The primary incumbent telecommunications provider in Turkey operates under **ASN 15924**. Intelligence regarding the network's external relationships indicates a diverse portfolio of transit providers, reflecting Turkey's strategic positioning between East and West.

Transit Relationships: ASN 15924 maintains direct transit relationships with major international and domestic operators. Notably, this includes: * **Global/Western Providers:** Vodafone Turkey, Cloudflare, and Accenture UK Limited. * **Asian/Chinese Providers:** Huawei Cloud and Zenlayer. * **Regional/Domestic Entities:** Turksat, Ihlas Net, and Euronet Telekomunikasyon.

Current intelligence indicates a lack of direct peering relationships for the incumbent ASN, relying instead on these transit arrangements for global reach [Internal Graph].

Physical Interconnection: In terms of physical infrastructure, several Turkish Autonomous Systems (ASNs) have established robust connections to international Internet Exchange Points (IXPs) and data centers. The top entities by physical connectivity include Gibirnet Iletisim Hizmetleri (18 connections), 3C1B Telekomunikasyon (13 connections), and Euronet Telekomunikasyon (11 connections) [Internal Graph]. Despite the market dominance of Türk Telekom, specific data regarding its top international upstream Tier 1 providers remains opaque in open-source reporting, highlighting a potential area of information control regarding critical upstream dependencies [Source 2] [Source 4].

1.3 Regional Connectivity and Geopolitical Alignments

Turkey's digital infrastructure strategy is deeply intertwined with its regional geopolitical ambitions, specifically the "Middle Corridor" initiative, which seeks to capitalize on transit routes between China and Europe.

The Black Sea and EU Integration: Turkey is a recognized partner in the European Union's strategy for a secure and resilient Black Sea region. This cooperation includes a specific "Connectivity Agenda" aimed at developing digital networks to link Europe with Central Asia, reinforcing Turkey's role as a transit hub [Source 1].

The Belt and Road Initiative (BRI): Turkey has engaged in a Memorandum of Understanding with China to align its Middle Corridor initiative with China's Belt and Road Initiative. This alignment suggests potential future investments in digital infrastructure that could deepen technological ties with Beijing, consistent with the presence of Huawei Cloud in the incumbent's

transit network [Source 3].

Regional Constraints: Despite its hub ambitions, Turkey's connectivity is constrained by persistent geopolitical frictions. There are no direct cross-border fiber optic connections with Armenia due to closed borders and the absence of diplomatic relations; consequently, Armenia relies on routing through Georgia and Iran [Source 3]. Furthermore, while Turkey borders landlocked nations such as Azerbaijan (Nakhchivan exclave), connectivity data regarding direct fiber links to Iran, Iraq, and Syria remains limited in open sources, often contingent on the volatile security environment in the southern border regions [Source 1].

References

- [Source 1] New EU strategy for secure, prosperous and resilient Black Sea region (https://enlargement.ec.europa.eu/news/new-eu-strategy-secure-prosperous-and-resilient-black-sea-region-2025-05-28_en)
- [Source 2] Balancing Security and Innovation: Opposition's View on Turkey's … (http://www.ifri.org/en/papers/balancing-security-and-innovation-oppositions-view-turkeys-digital-policies)
- [Source 3] OPINION - Techno-polar order and Türkiye's cybersecurity movement (https://www.aa.com.tr/en/opinion/opinion-techno-polar-order-and-turkiyes-cybersecurity-movement-the-struggle-for-digital-sovereignty/3627249)
- [Source 4] RIPE NCC - Internet Country Report: Türkiye (https://labs.ripe.net/media/documents/RIPE
- [Source 5] Expeditionary Capital in the Eastern Mediterranean: Why Turkey … (https://www.swp-berlin.org/publications/products/arbeitspapiere/CATS___Working_Paper_Nr_4_Je
- [Source 6] tepav The Economic Policy Research Foundation of Turkey - AWS (https://tepav.s3.eu-west-1.amazonaws.com/upload/files/1420818799-5.Strengthening_Connections_and
- [Source 7] Boosting the Internet in Landlocked Developing Countries (https://www.internetsociety.org/wp content/uploads/2017/10/LLDC_ExecSummary_20171004.pdf)
- [Internal Graph] Internal Knowledge Graph Intelligence (ASN and Connectivity Data)

Chapter 2

Infrastructure

Executive Summary

Turkey's telecommunications and digital infrastructure sector is characterized by ambitious state-directed targets contrasted with persistent rural coverage gaps and sovereignty challenges regarding data storage. The National Broadband Strategy has historically aimed for a 100% home-pass rate and high broadband usage, yet the infrastructure deployment remains uneven, particularly outside urban centers where a significant fiber coverage gap has rendered investment economically challenging for operators [Source 1 (PwC Strategy)][Source 5 (COMCEC)].

The fixed broadband market shows a fiber penetration rate of approximately 27.7%, with regulatory mechanisms such as "regulatory holidays" previously employed to incentivize the incumbent, Türk Telekom, to accelerate fiber rollout [Source 2 (Trade.gov)][Source 1 (PwC Strategy)]. Critical internet traffic exchange is centered around DE-CIX Istanbul; however, the efficiency of local traffic exchange is hampered by the restrictive peering policies of the primary operator, Türk Telekom [Source 2 (RIPE NCC)]. Furthermore, the lack of sufficient local hyperscale data center capacity forces a reliance on foreign cloud infrastructure, creating strategic vulnerabilities regarding data sovereignty and compliance with national data protection laws [Source 1 (Equinix)][Source 3 (LinkedIn)]. Future development is guided by high-level frameworks such as "Vision 2053" and the "Twelfth Development Plan (2024-2028)," though specific physical network expansion metrics within these plans remain opaque in open-source intelligence [Source 4 (UNDP)].

2.1 National Broadband and Fiber Optic Strategy

Turkey's infrastructure planning is driven by the National Broadband Strategy, which set aggressive targets to position the country as a regional digital hub. Key objectives included achieving a 100% home-pass rate for broadband and ensuring 80% broadband usage among the population aged 16-74 [Source 5 (COMCEC)]. To facilitate this, the government has utilized regulatory tools, such as exempting the incumbent operator, Türk Telekom, from certain market analy-

sis obligations (a “regulatory holiday”) to incentivize fiber investment until specific subscriber thresholds were met [Source 1 (PwC Strategy)].

Despite these ambitions, physical network expansion faces significant geographic and economic hurdles. Intelligence indicates a historical fiber coverage gap of approximately 57% in suburban and rural areas, where deployment has been deemed uneconomical for private operators [Source 1 (PwC Strategy)]. As of recent reporting, fiber penetration in Turkey stands at 27.7% [Source 2 (Trade.gov)]. The disparity between urban and rural infrastructure remains a critical obstacle to achieving the state’s goal of nationwide high-speed access and digital economy growth [Source 1 (PwC Strategy)].

2.2 Internet Exchange and Interconnection Architecture

The stability and efficiency of Turkey’s domestic internet traffic are heavily dependent on its Internet Exchange Points (IXPs). The primary active facility identified is DE-CIX Istanbul. While this facility serves as a crucial node for connectivity, its operational effectiveness is influenced by the peering policies of dominant market players. Specifically, Türk Telekom, the incumbent operator, maintains a peering policy described as not being open. This restrictive approach impacts the local internet landscape by potentially forcing domestic traffic to route through international pathways rather than exchanging locally, thereby affecting latency and resilience [Source 2 (RIPE NCC)].

2.3 Data Center Infrastructure and Sovereignty

Turkey’s data center landscape is currently undefined by a centralized public map of hyperscale facilities, though global providers such as Equinix maintain a presence in the market [Source 2 (Equinix)]. The sector faces a strategic challenge regarding data sovereignty. Due to a deficit in robust local hyperscale capacity, Turkish businesses often rely on cloud services hosted in foreign jurisdictions. This reliance introduces legal and security risks, as data stored abroad is subject to foreign laws (e.g., U.S. data access regulations) which may conflict with Turkish data privacy standards [Source 1 (Equinix)][Source 3 (LinkedIn)].

To mitigate these risks, there is a strategic imperative for the development of distributed infrastructure and local data centers. Increasing domestic capacity would allow data to remain within national borders, ensuring compliance with local regulations and reducing the “visibility gap” associated with public clouds hosted outside the country [Source 1 (Equinix)].

2.4 Mobile Network and Future Planning

Information regarding the specific geographical distribution of 5G coverage and mobile “white spots” in Turkey is limited in open sources. While global trends estimate 5G population coverage at roughly 15%, definitive data for Turkey’s current 5G penetration and specific spectrum auction results are not available in the analyzed intelligence [Source 1 (Nvidia)].

Looking forward, Turkey's infrastructure development is anchored in long-term state planning documents, specifically the "Twelfth Development Plan (2024-2028)" and "Vision 2053." These frameworks are intended to guide the country's recovery and development, particularly following major seismic events, and emphasize the necessity of digital skills and infrastructure restoration. However, detailed metrics regarding physical network expansion targets within these specific plans are not publicly detailed [Source 4 (UNDP)].

References

- [Source 1 (PwC Strategy)] Accelerating high-speed broadband in Turkey - PwC Strategy (https://www.strategyand.pwc.com/m1/en/reports/accelerating-high-speed-broadband-in-turkey-english.pdf)
- [Source 5 (COMCEC)] "Increasing Broadband Internet Penetration In the OIC Member … (https://www.comcec.org/wp-content/uploads/2021/07/9-TRA-PRO.pdf)
- [Source 2 (Trade.gov)] Turkey - Information and Communication Technology (https://www.trade.gov/country-commercial-guides/turkey-information-and-communication-technology)
- [Source 2 (RIPE NCC)] RIPE NCC - Internet Country Report: Türkiye (https://labs.ripe.net/media/docu
- [Source 2 (Equinix)] Equinix: Data Center Company & Enterprise Network Technologies (https://www.equinix.com/)
- [Source 1 (Equinix)] Data Sovereignty and AI: Why You Need Distributed Infrastructure (https://blog.equinix.com/blog/2025/05/14/data-sovereignty-and-ai-why-you-need-distributed-infrastructure/)
- [Source 3 (LinkedIn)] The Importance of Data Location: A Deep Dive into Data Sovereignty (https://www.linkedin.com/pulse/importance-data-location-deep-dive-sovereignty-diego-cervantes-knox)
- [Source 1 (Nvidia)] GeForce NOW Alliance Expands to Turkey, Saudi Arabia, Australia (https://blogs.nvidia.com/blog/geforce-now-alliance-pentanet/)
- [Source 4 (UNDP)] DP/DCP/TUR/5 - United Nations Development Programme (https://www.undp.org/sites/g/files/zskgke326/files/2025-07/turkiye-cdp-27-june.pdf)

Chapter 3

Market

Executive Summary

The Turkish telecommunications market is characterized by a dichotomy between competitive mobile data pricing and structural rigidities in infrastructure and device affordability. While Turkey ranks favorably in global mobile data pricing, placing 25th worldwide and offering lower costs than several Western European counterparts [Source 4], the sector struggles with the delayed deployment of next-generation networks. Unlike many peer nations, Turkey has not yet executed a widespread transition to 5G technology, continuing to rely on "4.5G" infrastructure [Source 2].

Market dynamics are heavily influenced by the incumbent, Türk Telekom, which retains a dominant position in fixed-line and broadband services. Despite privatization efforts, the sector exhibits signs of continued state influence and a lack of effective competition, which hampers aggressive market modernization [Source 1]. Furthermore, while service costs are relatively low, consumer access is constrained by high taxation on devices and modems, which offsets the benefits of affordable data plans [Source 1]. Investment activity in the broader Turkish market is rising, with a 33.8% increase in finalized M&A transactions reported in 2025, though specific consolidation within the telecom sector remains opaque [Source 5].

3.1 Competitive Landscape and State Influence

The competitive structure of the Turkish telecommunications market remains heavily skewed toward the incumbent operator, Türk Telekom. Intelligence indicates that despite the formal privatization of the entity, Türk Telekom maintains a dominant market share in fixed-line and broadband services [Source 1]. The regulatory environment has been described as lacking effective enforcement to foster robust competition, with the incumbent maintaining close ties to the government [Source 1].

This structural dominance has resulted in a market environment where price wars are less evident than in more fragmented European markets. While global trends point toward commoditization

and falling Average Revenue Per User (ARPU) [Source 1], specific data on ARPU trends and subscriber market shares for Turkey's top operators remains unavailable in current open-source reporting, suggesting a degree of opacity in operator performance metrics.

3.2 Infrastructure and Technology Status

A critical lag in Turkey's telecommunications development is the absence of widespread 5G deployment. While global markets are increasingly adopting 5G standards to support lower latency and higher capacity, Turkey continues to utilize LTE-Advanced technology, marketed locally as "4.5G" [Source 2]. Public sentiment and technical discussions indicate frustration with this delay, with the continued reliance on 4.5G viewed by some segments as a stagnation of technological progress [Source 2].

Consequently, there is no available data comparing 5G performance to 4G within the country, as the infrastructure upgrade has not been fully realized. This delay places Turkey behind the technological curve relative to nations that have already operationalized 5G networks to support advanced industrial and consumer applications.

3.3 Pricing, Affordability, and Consumer Economics

Turkey occupies a competitive position regarding the raw cost of mobile data. The country ranks 25th globally for the average price of 1GB of mobile data, placing it ahead of nations such as Ireland [Source 4]. Regional analysis suggests that data costs in Eastern Europe, a proxy region for Turkey's pricing tier, average approximately USD 1.27 per 1GB, significantly lower than the Western European average of USD 2.08 [Source 2].

However, affordability is complex when broader economic factors are considered. The Turkish government utilizes a Universal Service Fund intended to subsidize access for underserved regions and bridge the digital divide [Source 1]. Despite these subsidies and low service costs, the total cost of ownership for consumers is inflated by high taxation on Information and Communication Technology (ICT) hardware. The tax burden on smartphones, modems, and computers significantly reduces overall affordability, creating a demand gap where households that could theoretically afford monthly service fees are barred from entry due to hardware costs [Source 1].

3.4 Investment and M&A Activity

The broader Turkish economic landscape is experiencing a surge in merger and acquisition (M&A) activity. In 2025, the number of finalized M&A transactions in Turkey increased by 33.8% compared to the previous year, with a total transaction volume reaching approximately TRY 574 billion [Source 5]. While this indicates a robust environment for capital movement and corporate restructuring within the country, current intelligence does not confirm specific, high-impact consolidation activities or hostile takeovers directly within the telecommunications

sector. The activity appears distributed across various industries, including technology and energy, rather than being concentrated solely on telecom operators [Source 5].

References

- [Source 1] Why Turkey's Telecommunications Sector Is Not Keeping Pace with Demand (https://freedomhouse.org/sites/default/files/Infrastructure%20and%20Independence%20-%20Why%20Turkeys%20Telecomms%20Sector%20is%20Not%20Keeping%20Pace%20with%20Demand.p
- [Source 2] The Cost of 1GB Of Mobile Data in 237 Countries - Broadband Deals (https://bestbroadbanddeals.co.uk/mobiles/worldwide-data-pricing/)
- [Source 3] r/Turkey on Reddit: Why haven't we switched to 5G yet… (https://www.reddit.com/r/Turkey/c
- [Source 4] How do mobile data prices in Ireland compare to other EU countries? (https://www.recharge.com/blog/en-gb/ie/how-expensive-is-mobile-data-in-ireland)
- [Source 5] The 2025 Mergers and Acquisitions Outlook Report has been Published - Gide (https://www.gide.com/en/news-insights/the-2025-mergers-and-acquisitions-outlook-report-has-been-published/)
- [Source 6] Accelerating high-speed broadband in Turkey - PwC Strategy (https://www.strategyand.pwc.co high-speed-broadband-in-turkey-english.pdf)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 4

Localization

4.1 Executive Summary

Turkey exhibits a "Very High" level of e-government development, with an E-Government Development Index (EGDI) score of 0.7900 [1]. Despite this digital maturity, the nation faces significant strategic challenges regarding data sovereignty and localization. The Turkish government has enacted specific legislation, notably amendments to Law No. 5651, to mandate the local storage of user data by major social network providers [2]. However, the broader landscape of cloud infrastructure remains opaque; there is a notable absence of definitive public data regarding the market share of hyperscale providers (AWS, Azure, Google) versus local hosting solutions [3], or the percentage of internet traffic exchanged locally via Internet Exchange Points (IXPs) [4]. Furthermore, Turkish entities utilizing foreign cloud services face legal risks from extraterritorial regulations such as the U.S. CLOUD Act, which threatens to bypass Turkish data protection frameworks and undermine national sovereignty [5].

4.2 Legal Framework and Data Localization Mandates

Turkey has moved beyond voluntary localization to enforceable legal mandates, specifically targeting social media platforms. Under amendments to the Social Media Law (Law No. 5651), foreign and domestic social network providers with more than 1 million daily accesses in Turkey are legally obligated to store user data within the country [2]. The Information and Communication Technologies Authority (ICTA) has reinforced this by issuing secondary regulations requiring these providers to prioritize the storage of users' basic information and ICTA-mandated data within Turkey [2]. This requirement specifically applies to citizens residing in Turkey, excluding those living abroad [2].

While these laws are stringent for social media, intelligence indicates a lack of publicly available official strategies regarding the exclusive use of national cloud services for broader public administration or critical infrastructure [6]. There is currently no definitive evidence of prominent Turkish companies or government agencies publicly committing to exclusively local hosting

solutions for data sovereignty reasons [7].

4.3 Strategic Risks: Extraterritoriality and Sovereignty

The reliance of Turkish entities on foreign cloud infrastructure introduces significant legal and national security vulnerabilities. The primary threat stems from the extraterritorial application of foreign laws, such as the U.S. CLOUD Act. This legislation allows U.S. law enforcement to compel U.S.-based cloud providers to disclose data regardless of its physical storage location, effectively bypassing Turkish sovereignty [5].

Key strategic implications include: * **Undermined Sovereignty:** The CLOUD Act permits foreign access to data generated within Turkey without the consent of Turkish authorities, challenging the state's control over its information environment [8]. * **Privacy Protection Gaps:** Such extraterritorial reach creates a "protection gap," where Turkish citizens' data may be disclosed without adhering to Turkish privacy standards or consent requirements [5]. * **National Security:** Foreign government access to data stored by Turkish entities on global clouds could be exploited for espionage or to influence Turkish policy, creating a vector for "digital colonialism" [9].

4.4 Digital Identity and Infrastructure Maturity

Turkey's digital infrastructure supports a robust e-government ecosystem, yet specific metrics on national adoption remain limited. * **Digital Identity:** Turkey utilizes the `.name.tr` domain extension to foster personal digital identities. This domain is restricted to Turkish citizens or residents and supports Internationalized Domain Names (IDNs), accommodating local linguistic needs [10]. However, there is insufficient data to determine the broader adoption rate of the `.tr` ccTLD compared to generic gTLDs [11]. * **Infrastructure Visibility:** While Turkey possesses local interconnection infrastructure, such as the DE-CIX presence in Istanbul, there is no definitive data available to quantify the percentage of internet traffic exchanged locally versus routed internationally [4]. Similarly, the specific hosting locations of top Turkish websites—whether on domestic data centers or foreign clouds—cannot be determined from open sources [12].

4.5 References

- [1] E-Government Survey 2022 (https://desapublications.un.org/sites/default/files/publications/2022-09/Web%20version%20E-Government%202022.pdf)
- [2] Turkish data localization rules in effect for social media companies (https://iapp.org/news/a/turkish-data-localization-rules-in-effect-for-social-media-companies)
- [3] Public cloud revenue: Spending boom for AWS, Azure and Google (https://www.techmonitor.ai/cloud/cloud-revenue-aws-azure-google-cloud/)

- [4] Internet Exchange Points - Euro-IX (https://www.euro-ix.net/media/filer_public/ab/d7/abd70b77-5b42-4c32-af47-7114e9a3c340/ixp_report_2020_.pdf)
- [5] Digital Privacy Rights and CLOUD Act Agreements - BrooklynWorks (https://brooklynworks.brooklaw
- [6] Critical infrastructure and the cloud: Policy for emerging risk (https://www.atlanticcouncil.org/in-depth-research-reports/report/critical-infrastructure-and-the-cloud-policy-for-emerging-risk/)
- [7] Sovereignty and Data Localization - Belfer Center (https://www.belfercenter.org/publication/sovereign and-data-localization)
- [8] LEGAL ACCESS TO THE GLOBAL CLOUD - Columbia Law Review (https://columbialawreview.org access-to-the-global-cloud/)
- [9] Sovereignty and Data Localization - Belfer Center (https://www.belfercenter.org/publication/sovereign and-data-localization)
- [10] .NAME.TR domain name registration | Turkey - EuroDNS (https://www.eurodns.com/domain-extensions/name.tr-domain-registration)
- [11] Middle East and Adjoining Countries DNS Study | ICANN (https://www.icann.org/en/system/files/fi dns-study-26feb16-en.pdf)
- [12] Equinix: Data Center Company & Enterprise Network Technologies (https://www.equinix.com/)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 5

Security

5.1 Security

Executive Summary

Turkey's national security posture regarding the digital domain is characterized by a stark contrast between high-level governance metrics and operational opacity. Globally, Turkey is recognized as a top-tier cyber power, achieving a perfect score on the ITU Global Cybersecurity Index (GCI), which positions the nation as a role model in legal, technical, and organizational cybersecurity commitments [Source 2] [Source 3]. This strategic commitment is operationally supported by robust adoption of security protocols among major telecommunications providers; notably, all top 10 Autonomous System Numbers (ASNs) by population reach support DNSSEC [IYP-GRAPH].

However, this high-level readiness is obscured by a significant lack of publicly verifiable data regarding operational resilience and specific threat landscapes. The National Cyber Security Index (NCSI) highlights a lack of publicly available evidence concerning cyber crisis management plans and digital forensics capabilities [Source 2]. Furthermore, while the nation has invested heavily in defense following historical large-scale attacks, there is a dearth of current, open-source intelligence regarding specific DDoS volumes, malware infection rates, or the technical response capabilities of the national CERT/CSIRT [Source 1]. Critical infrastructure remains vulnerable due to reliance on legacy SCADA systems and a shortage of qualified cybersecurity personnel [Source 1] [Source 3].

5.2 National Cybersecurity Governance and Maturity

Turkey has established a formidable governance framework for cybersecurity. The International Telecommunication Union (ITU) ranks Turkey in "Tier 1" of its Global Cybersecurity Index, awarding it a score of 100/100. This ranking reflects strong performance across five pillars: legal measures, technical measures, organizational measures, capacity building, and cooperation

[Source 2] [Source 3].

Despite this perfect score, independent assessments suggest a gap between policy existence and public transparency. The National Cyber Security Index (NCSI) notes that while frameworks may exist, there is often no "publicly available evidence" to validate the implementation of key indicators. Specific areas lacking transparency include requirements for cryptosystems, electronic registered delivery services, and the operational details of cyber operations units [Source 2]. This opacity complicates external assessments of Turkey's actual operational readiness to handle systemic cyber crises.

5.3 Network Infrastructure and Protocol Security

The structural integrity of Turkey's internet backbone appears robust, particularly regarding the adoption of Domain Name System Security Extensions (DNSSEC) among major providers. Intelligence indicates that 100% of the top 10 ASNs by population reach—including major entities such as TTNet (Turk Telekom), Superonline, and Vodafone Turkey—support DNSSEC [IYP-GRAPH]. This widespread adoption mitigates the risk of DNS spoofing and cache poisoning attacks for a vast majority of the Turkish population.

Regarding routing security and the Border Gateway Protocol (BGP), the available data suggests a clean peering environment. Analysis of the dependency graph reveals that zero Turkish ASNs are currently peering with upstream providers identified as "unverified" or "potentially untrusted" [IYP-GRAPH]. While specific RPKI validation rates remain unquantified in the provided intelligence, the absence of flagrant peering risks and the strategic alignment with global standards like MANRS (Mutually Agreed Norms for Routing Security) suggested by APNIC's reporting frameworks indicate a maturing routing security posture [Source 4].

5.4 Critical Infrastructure Vulnerabilities

Turkey's critical infrastructure (CI) sectors face systemic vulnerabilities driven by technological legacy and human capital deficits. Reports from researchers affiliated with Turkish institutions highlight that the continued reliance on older, proprietary SCADA systems—originally designed without security in mind—constitutes a primary weakness [Source 1]. As these systems become increasingly automated and interconnected with the broader internet, the attack surface expands significantly.

Key vulnerabilities identified include: * **Legacy Systems:** Operational Technology (OT) environments are often outdated and lack security-by-design principles [Source 1]. * **Human Factors:** Non-technical vulnerabilities, such as the propagation of malware via USB drives and insufficient security training, remain critical weak points [Source 1]. * **Resource Shortages:** There is a documented shortage of qualified cybersecurity experts within the country, coupled with a lack of information-sharing culture between public and private sectors [Source 3]. * **Maturity Gaps:** A disparity exists between the private sector and governmental entities, with

public sector infrastructure often lagging in risk management maturity [Source 3].

5.5 Threat Landscape and Operational Opacity

Current intelligence regarding the specific volume and nature of cyber threats targeting Turkey is limited, likely due to strict information controls or a lack of reporting to global monitoring bodies. There is no definitive open-source statistical data available regarding recent DDoS attack volumes or specific malware infection rates for the current period [Source 4] [Source 2].

While historical data from 2016 indicated high malware infection rates (approx. 41%), current metrics are unavailable [Source 2]. Similarly, while it is known that Turkey has suffered large-scale cyber attacks in the past which spurred investment, there are no publicly available technical reports detailing the specific capabilities of the national CERT/CSIRT in responding to sophisticated nation-state intrusions [Source 1]. This absence of data prevents a granular assessment of the current threat tempo but suggests a national strategy of operational secrecy regarding cyber defense activities.

References

- [Source 1] CYBER CAPABILITIES AND NATIONAL POWER Volume 2 (https://www.iiss.org/globalass library—content–migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2.pdf)
- [Source 2] NCSI :: Türkiye - National Cyber Security Index (https://ncsi.ega.ee/country/tr_2022/)
- [Source 3] Global Cybersecurity Index 2024 - ITU (https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf)
- [Source 4] Annual Report - APNIC (https://www.apnic.net/wp-content/uploads/2025/02/APNIC-AR-2024.pdf)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 6

Governance

Executive Summary

Turkey's governance of the digital and information domains is characterized by a dualistic framework: while legislative efforts are underway to align data protection standards with European Union models, the operational reality reflects a trajectory toward centralized state control akin to the "Beijing Model." The legal environment is defined by the extensive powers of the Information and Communication Technologies Authority (BTK), which lacks robust independence from executive influence, raising concerns regarding political interference in regulatory processes [Source 1].

Although Turkey has enacted Law No. 6698 on the Protection of Personal Data (PDPL) and recently amended it to bridge gaps with the GDPR, exemptions for national security and law enforcement create significant vulnerabilities regarding state surveillance [Source 2][Source 3]. The state retains broad authority to intercept communications and restrict content under Law No. 5651 and the 2022 "Disinformation Law," which criminalizes the dissemination of "misleading information" and expands liability for social media platforms [Source 4][Source 5]. Furthermore, Turkey's non-ratification of the Budapest Convention on Cybercrime limits its capacity for standardized international cooperation in evidence gathering and mutual legal assistance [Source 6].

6.1 Regulatory Framework and Independence

The primary regulatory body for telecommunications and internet governance is the Information and Communication Technologies Authority (BTK). Intelligence assessments indicate that the current legal framework insufficiently protects the BTK from presidential and governmental influence. European Commission reports highlight that the regulatory environment is susceptible to undue political interference, compromising the objectivity of decision-making processes [Source 1].

This lack of autonomy extends to market regulation. The telecommunications sector operates

under a transitional legal framework that has not fully aligned with EU competition directives. Evidence suggests that the regulatory structure has failed to ensure a fully open market, evidenced by the state-owned Türksat's monopoly on satellite services for public administration and delays in 5G spectrum allocation [Source 7][Source 8]. These factors create an environment where regulatory mechanisms may be utilized to restrict competition or favor incumbent operators rather than promoting a fair digital economy.

6.2 Data Protection and Privacy Legislation

Turkey's data governance is anchored in Law No. 6698 on the Protection of Personal Data (PDPL), modeled after the EU's 1995 Data Protection Directive. Recent amendments, effective June 1, 2024, aim to align the PDPL more closely with the General Data Protection Regulation (GDPR), particularly regarding the processing of special categories of data and cross-border data transfers [Source 2][Source 3].

The Personal Data Protection Authority (KVKK) serves as the enforcement body, possessing the power to impose administrative fines and halt data processing. The KVKK has demonstrated proactive enforcement through the mandatory VERBIS registration system for data controllers and has issued guidelines on artificial intelligence to protect fundamental rights [Source 9][Source 10]. However, the efficacy of these protections against state intrusion is limited. National security and law enforcement authorities are often exempted from specific legal frameworks regarding data processing, relying instead on broad constitutional limits that may lack sufficient procedural safeguards [Source 11].

6.3 Surveillance and State Control of Information

The legal architecture governing surveillance balances constitutional privacy guarantees against expansive national security laws. Law No. 2937 (National Intelligence Organization Law) and Law No. 5651 (Internet Law) authorize surveillance and content restriction for reasons of public order and national security [Source 12]. While judicial oversight is technically mandated, the independence of the judiciary is questioned, and emergency decrees have historically granted the government unrestricted access to communications data without court orders [Source 13].

Turkey's approach to internet governance increasingly mirrors authoritarian models emphasizing state sovereignty over digital rights. This is exemplified by the "Disinformation Law" (October 2022), which amended the Turkish Penal Code to criminalize the "public dissemination of misleading information." This legislation grants the BTK authority to throttle internet bandwidth for non-compliant social media platforms and mandates strict data localization and local representation for tech companies [Source 5]. These measures have contributed to a "Partly Free" designation in internet freedom assessments, citing obstacles to access and limits on content as key drivers [Source 14].

6.4 International Cooperation on Cybercrime

Turkey has not ratified the Council of Europe Convention on Cybercrime (Budapest Convention) or the African Union Convention on Cyber Security (Malabo Convention) [Source 6][Source 15]. The absence of ratification creates distinct challenges for international judicial cooperation. Without the standardized legal frameworks provided by the Budapest Convention, Turkey relies on ad-hoc diplomatic channels for mutual legal assistance (MLA). This status complicates the cross-border acquisition of electronic evidence and limits Turkey's influence in shaping international cybercrime norms, potentially hindering investigations into transnational cyber threats [Source 6].

References

- [Source 1] 20161109_report_turkey.pdf (https://enlargement.ec.europa.eu/document/download/e703a76 bf7f-46d1-8a13-6a836683e838_en?filename=20161109_report_turkey.pdf)
- [Source 2] GDPR Countries in 2026 | GDPR Advisor (https://www.gdpradvisor.co.uk/gdpr-countries)
- [Source 3] Turkey's data protection amendments for 2024: A closer look | IAPP (https://iapp.org/news/a/turkeys-data-protection-amendments-for-2024-a-closer-look)
- [Source 4] TÜRKİYE'S "DISINFORMATION LAW" TIGHTENS GOVERNMENT CONTROL (https://www.amnesty.org/es/wp-content/uploads/2022/10/EUR4461432022ENGLISH.pdf)
- [Source 5] Turkey: Dangerous, Dystopian New Legal Amendments (https://www.hrw.org/news/2022/10/ dangerous-dystopian-new-legal-amendments)
- [Source 6] The Budapest Convention on Cybercrime: benefits and impact (https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac)
- [Source 7] Screening report Turkey - Chapter 10 – Information Society and Media (https://enlargement.ec.europa.eu/document/download/346e0a58-f1d9-4333-ae3f-725b1d4e9f37_en?filename=screening_report-10-tr_internet_en.pdf)
- [Source 8] Telecoms and Media Turkey | Srp-Legal (https://www.srp-legal.com/wp-content/uploads/2022/07/2022-Telecoms-and-Media-Turkey.pdf)
- [Source 9] Mandatory data protection compliance in Turkey: VERBIS (https://www.ibanet.org/Mandator data-protection-compliance-Turkey-VERBIS)
- [Source 10] AI Watch: Global regulatory tracker - Turkey (https://www.jdsupra.com/legalnews/ai-watch-global-regulatory-tracker-9711736/)
- [Source 11] Government access to data in third countries II (https://www.edpb.europa.eu/system/files/202 10/study_on_government_access_to_data_in_third_countries_17042023_mexico_and_turkiye_final
- [Source 12] Surveillance Law of Turkey in a Digital Age (https://www.bicakhukuk.com/en/surveillance-law-of-turkey-in-a-digital-age/)
- [Source 13] Turkey Doubles Down on Violations of Digital Privacy (https://www.eff.org/deeplinks/2020/1 doubles-down-violations-digital-privacy-and-free-expression)
- [Source 14] FREEDOM ON THE NET 2012: GLOBAL SCORES (https://www.freedomhouse.org/sites/d %20Tables%20and%20Charts%20FINAL.pdf)

- [Source 15] T-CY assessment report: The mutual legal assistance provisions (https://rm.coe.int/16802e726c)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 7

Strategic Synthesis & Roadmap

Chapter 8

Section 7: Strategic Synthesis & Roadmap

TO: The Office of the President / Prime Minister **FROM:** Office of the Chief Strategy Officer **SUBJECT:** The "Digital Bosphorus" Doctrine – Operationalizing Sovereignty **DATE:** October 26, 2025

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

8.1.1 The Narrative: The Fortress and the Bridge

Turkey stands at a critical juncture. We have successfully digitized the state (E-Government) and secured the perimeter (Tier 1 ITU ranking, DNSSEC adoption). We have positioned ourselves geopolitically as the "Middle Corridor"—a digital bridge between a regulating Europe and a rising Asia. However, our ambition to be a global digital power is currently outpacing our physical capabilities. We are attempting to enforce a "Beijing Model" of sovereign control over an infrastructure that is still reliant on Western transit and legacy technology.

8.1.2 The Paradox: Sovereignty without Autonomy

The central contradiction in our current posture is **Legislative Sovereignty vs. Infrastructural Dependency.** We have passed laws demanding data localization (Law No. 5651) and digital borders, yet we lack the domestic hyperscale cloud capacity to house that data, forcing our businesses into foreign jurisdictions (and under the thumb of the U.S. CLOUD Act). We demand a cutting-edge economy, yet we tax the hardware (modems/phones) required to access it, and we have allowed the incumbent (Türk Telekom) to delay the fiber and 5G rollout essential for future growth. We have built a legal fortress on a foundation of copper.

8.2 2. SWOT Analysis: The Strategic Cheat Sheet

STRENGTHS (Internal)	WEAKNESSES (Internal)
Geostrategic Location: The physical and digital bridge between EU and Asia (Middle Corridor).	**Infrastructure Lag:** 5G is delayed; Fiber penetration (27%) is too low for an industrial power.
E-Gov Maturity: High citizen adoption (0.79 EGDI) and strong digital identity foundations.	**Cloud Deficit:** Lack of local hyperscale data centers makes data localization laws hard to enforce.
Cyber Hygiene: Excellent DNSSEC adoption (100% among top telcos) and strong governance frameworks.	**Incumbent Lethargy:** Türk Telekom's dominance and restrictive peering stifle innovation and speed.

OPPORTUNITIES (External)	THREATS (External)
Nearshoring: EU companies moving digital operations closer; Turkey can be their data hub.	**The "Techno-Polar" Trap:** Being forced to choose between US (Silicon Valley) and Chinese (Huawei) tech stacks.
Sovereign Cloud: Building a National Cloud PPP to capture the value of data currently leaking abroad.	**Extraterritoriality:** U.S. CLOUD Act bypassing Turkish sovereignty to access citizen data.
Black Sea Connectivity: Leveraging EU funding for subsea cables to bypass hostile neighbors.	**Legacy SCADA:** Critical infrastructure relies on outdated OT systems vulnerable to state-sponsored sabotage.

8.3 3. Strategic Roadmap: The Policy Agenda

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

Objective: Secure the Perimeter & Unblock the Market

1. **The "Data Haven" Decree:** Immediately incentivize the construction of Tier IV hyperscale data centers through tax holidays and energy subsidies. We cannot enforce data localization if there is nowhere local to store the data.
2. **Critical Infrastructure Audit:** Mandate a "Zero Trust" security audit for all SCADA/OT systems in energy and water sectors. The reliance on legacy systems is a national security risk that must be quantified immediately.
3. **Hardware Tax Reform:** Reduce the Special Consumption Tax (ÖTV) on modems and 5G-enabled devices. We are currently taxing the tools of our own economic liberation.

8.3.2 Phase 2: Structural Reforms (12 - 36 Months)

Objective: Build the "Digital Bosphorus"

1. **Fiber Unleashed:** End the "Regulatory Holidays" for the incumbent. Enforce strict "Dig Once" policies and open-access duct sharing. If Türk Telekom will not build fiber to the rural edges, allow municipalities and private competitors to do so without bureaucratic friction.
2. **5G Spectrum Auction:** Launch the 5G spectrum auction with a **"Secure Vendor" clause**. Balance our geopolitical ties by allowing a mix of vendors (e.g., Ericsson/Nokia for core, Huawei for radio) to prevent total vendor lock-in while ensuring speed.
3. **Sovereign Cloud Partnership:** Establish a Public-Private Partnership (PPP) to create a "Turkish National Cloud." This entity will host all critical government data and offer compliant hosting for the private sector, effectively neutralizing the U.S. CLOUD Act threat.

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

Objective: Regional Hegemony

1. **The Regional Data Exchange:** Position Istanbul not just as a transit point, but as the primary Internet Exchange Point (IXP) for the Middle East, Balkans, and Caucasus. Traffic should settle *in* Turkey, not just flow *through* it.
2. **Cyber-Diplomacy:** Since we have not ratified the Budapest Convention, we must establish a network of bilateral "Digital Mutual Assistance Treaties" with key trade partners to manage cybercrime without ceding sovereignty.
3. **Human Capital Export:** Transform our cyber workforce shortage into a surplus by integrating cybersecurity curricula into high school vocational tracks, aiming to become a net exporter of cyber-talent to the region.

8.4 4. Final Verdict

8.4.1 Investability Score: MEDIUM

- **Explanation:** Turkey offers immense volume and a strategic location that cannot be ignored. However, the market is distorted by heavy state intervention, an opaque regulatory environment (BTK independence issues), and currency volatility. Investors will come for the demographics but hesitate due to the "rules of the game" changing unpredictably.

8.4.2 Maturity Score: DEVELOPING (High-Potential)

- **Explanation:** We are "Mature" in governance (laws, e-gov, security protocols) but "Developing" in physical reality (fiber depth, 5G, cloud capacity). We have a First World

government operating on Second World infrastructure. Bridging this gap is the primary task of the next administration.