STRATEGIC COUNTRY REPORT: FRANCE

Automated Strategic Analyst (v2.2 Parallel)

03 February 2026

Contents

Chapter 1

Geopolitics

Executive Summary

France's geopolitical posture in the digital domain is defined by a tension between ambitious state-led doctrines of "digital sovereignty" and significant underlying technical dependencies on foreign infrastructure. Paris views digital sovereignty not merely as a regulatory framework for protecting rights, but as a geoeconomic imperative to ensure the capacity to act autonomously in the political and economic spheres [Source 1]. This strategy is operationalized through substantial state investments, such as the €54 billion "France 2030" initiative, and rigorous regulatory standards like SecNumCloud [Source 1 (Q14)].

However, intelligence analysis of France's network topology reveals a critical vulnerability: a disproportionate reliance on foreign Tier 1 transit providers. Specifically, French Autonomous Systems (ASNs) exhibit a massive upstream dependency on the US-based operator Cogent Communications (AS174), creating a potential strategic chokepoint [Internal Graph]. While France maintains strong industrial leverage in the physical layer through global leaders like Alcatel Submarine Networks [Source 1 (Q6)], its logical layer connectivity remains heavily intertwined with non-European entities, complicating its goal of complete strategic autonomy.

Strategic Doctrine: Digital Sovereignty and Autonomy

France has positioned itself as a primary architect of the European approach to digital sovereignty. The French strategic outlook has evolved from a focus on civil liberties to a broader "Geopolitics of the Datasphere," where control over digital infrastructure is equated with national power [Source 1]. This doctrine aims to enable democratic societies to act resiliently and autonomously, rejecting the notion of sovereignty as purely a fixed state in favor of a dynamic capability to shape the digital future [Source 1].

To support this doctrine, the French government has implemented a multi-layered policy framework: * **Investment in Strategic Capabilities:** The "France 2030" plan allocates capital to emerging technologies, digital security, and industrial 5G applications, aiming to reduce produc-

tion taxes and regain economic independence [Source 1 (Q14)][Source 4 (Q14)]. * **Regulatory Protectionism:** The "Trusted Cloud Strategy" mandates that government agencies and critical commercial entities utilize services certified under the SecNumCloud scheme. This certification, maintained by the national cyber security authority (ANSSI), imposes strict security requirements that effectively shield sensitive data from foreign legal jurisdictions and cloud providers [Source 1 (Q14)]. * **Cyber Defense:** The National Cyber Security Strategy (2015) and subsequent updates prioritize the protection of national sovereignty and the elevation of digital security as a competitive advantage for French enterprise [Source 2 (Q14)].

Network Topology and Critical Dependencies

Despite the political emphasis on autonomy, technical analysis of France's internet routing architecture identifies severe dependencies on foreign infrastructure. Network graph analysis highlights that Cogent Communications (AS174), a US-based Tier 1 operator, holds a dominant position in France's upstream transit market.

- **The Cogent Chokepoint:** Data indicates 39,993 incoming `DEPENDS_ON` relationships from French ASNs to COGENT-174. This volume of dependency far outstrips other providers, suggesting that a significant portion of French domestic and international traffic relies on this single foreign entity for transit [Internal Graph].
- **Critical Operator Vulnerability:** High `d.hege` scores (indicating a dependency score of 1.0 or 100%) were observed for major French telecommunications and infrastructure entities. Critical ASNs, including those belonging to **Orange S.A.**, **OVH SAS**, **SFR**, **Bouygues Telecom**, and the academic research network **RENATER**, exhibit instances of total dependency on specific upstream providers [Internal Graph].
- **Localized Risks:** The analysis further identified 100% dependency relationships between specific entities, such as CDN77 and CDNEXT, indicating localized vulnerabilities where service disruption could occur if the primary transit link is severed [Internal Graph].

This topology suggests that while France exercises sovereignty over policy and physical territory, its "logical" sovereignty—the routing of data—is heavily constrained by reliance on non-domestic transit networks.

Industrial Capabilities and Global Connectivity

France retains significant geopolitical leverage through its industrial base and physical connectivity assets. The country is physically aligned with the European digital bloc, serving as a critical north-south connector for traffic originating from Africa and destined for European hubs [Source 1 (Q8)].

- **Submarine Cable Leadership:** France is home to Alcatel Submarine Networks (ASN), a global leader in the manufacturing, installation, and maintenance of submarine optical systems [Source 1 (Q6)]. As geopolitical tensions rise regarding the control of sub-

sea cables—particularly efforts to exclude Chinese vendors from global infrastructure—France's indigenous capacity to deploy and repair these critical assets provides it with strategic influence independent of US or Asian supply chains [Source 2 (Q6)].

- **Infrastructure Investment:** Major domestic operators like Orange are heavily investing in new-generation digital infrastructure, including fiber and 4G/5G networks across Europe. This investment supports the "France Relance" recovery plan's objective of upgrading production facilities and ensuring connectivity resilience [Source 1 (Q10)][Source 4 (Q14)].

References

- [Source 1] Digital sovereignty – new empires, big tech and geopolitics | FAU (https://www.fau.eu/2025/11/news/research/digitale-souveraenitaet-neue-imperien-big-tech-und-geopolitik/)
- [Source 1 (Q6)] Alcatel Submarine Networks – We connect the world (https://www.asn.com/)
- [Source 1 (Q8)] Digital Corridors: The Africa Connection - The Equinix Blog (https://blog.equinix.com/blog/2022/02/09/digital-corridors-the-africa-connection/)
- [Source 1 (Q10)] Session 2021 - Rapport annuel intégré - Orange.com (https://rai.orange.com/en/iar2021/)
- [Source 1 (Q14)] France - Digital Economy - International Trade Administration (https://www.trade.gov/country-commercial-guides/france-digital-economy)
- [Source 2 (Q6)] Subsea cables: how the US is pushing China out of the internet's … (https://ig.ft.com/subsea-cables/)
- [Source 2 (Q14)] France and cyber security - Ministry for Europe and Foreign Affairs (https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/)
- [Source 4 (Q14)] France Relance recovery plan: building the France of 2030 (https://www.diplomatie.gouv.fr/en/french-foreign-policy/economic-diplomacy-foreign-trade/promoting-france-s-attractiveness/france-relance-recovery-plan-building-the-france-of-2030/)
- [Internal Graph] Internal Knowledge Graph (ASN Dependency and RPKI Analysis)

Chapter 2

Infrastructure

Executive Summary

France exhibits a mature fixed broadband infrastructure, characterized by a high penetration rate of Fiber to the Home (FTTH) technology. As of June 2025, FTTH accounts for 79% of all fixed internet subscriptions, driven by the national "France Très Haut Débit" strategy which targets universal fiber availability [Source 5]. Despite this success in fixed lines, intelligence regarding the granular distribution of hyperscale data centers and specific 5G population coverage remains opaque in open sources. While the European Union aggregate data suggests high 5G household coverage, specific French metrics and high-band spectrum deployment figures are currently unavailable [Source 3]. The resilience of France's digital infrastructure is heavily contingent on the stability of the electrical grid; recent analysis of storm impacts indicates that power shortages are the primary cause of mobile site unavailability during natural disasters, rather than direct physical damage to telecommunications assets [Source 7].

2.1 Fixed Broadband and Fiber Optic Deployment

France has achieved significant milestones in the deployment of high-speed fixed connectivity. As of June 2025, the FTTH penetration rate stands at 79% of all fixed plan subscriptions, representing approximately 25.7 million internet subscriptions to a fiber plan [Source 5]. This deployment aligns with the "France Très Haut Débit" National Broadband Plan, which established a strategic target to provide fiber connectivity for the entire population by 2025 [Source 6].

However, geographical disparities persist. Intelligence indicates that while national targets are ambitious, the deployment of fiber optics faces inherent challenges in rural and less populated areas. Low population density and the distance to core network facilities in these regions act as significant obstacles to adoption and deployment [Source 8]. Historical analysis suggests that while France emphasized Fiber-to-the-Premises (FTTP), it has faced challenges in achieving uniform high performance across all territories compared to other deployment models [Source

11].

2.2 Mobile Network Infrastructure and 5G

Current intelligence on the specific status of 5G deployment in France is limited. While the European Union as a whole reports a 94.3% 5G household coverage rate (NSA and SA) as of the end of 2024, specific figures for France's population coverage and high-band (mmWave) spectrum deployment are not definitively reported in available technical findings [Source 3]. Furthermore, reports indicate that the current state of play regarding the authorization of 5G bands in the region shows limited progress compared to previous assessment periods [Source 3].

Regarding specific spectrum assets, the 2.6 GHz Time Division Duplex (TDD) band is available in France for local Private Mobile Radio (PMR) like services, facilitating specific industrial or local connectivity needs [Source 10]. However, data regarding the outcomes of recent mobile spectrum auctions for wider commercial 4G and 5G bands is currently unavailable in open sources.

2.3 Internet Exchange and Interconnection

France serves as a significant interconnection hub for Europe, primarily through France-IX. The exchange points in Paris and Marseille are active, with France-IX reporting over 500 members. These facilities interconnect several hundred organizations, including carriers, Internet Service Providers (ISPs), and content and cloud infrastructure providers [Source 4].

Despite the strategic importance of these nodes, granular traffic statistics and specific Autonomous System Number (ASN) counts for French IXPs are not publicly transparent. Intelligence suggests that data accuracy relies heavily on self-reporting by individual IXPs, and comprehensive traffic statistics are not consistently available for analysis [Source 12].

2.4 Infrastructure Resilience and Vulnerabilities

The resilience of France's internet infrastructure is critically linked to its energy sector. Analysis of network performance during natural disasters reveals significant dependencies. For instance, during Storm Ciaran in November 2023, 90% of the unavailable mobile sites in France were attributed to electricity shortages. Only 10% of failures were due to direct physical issues such as antenna disorientation or access difficulties [Source 7].

This dependency highlights a primary physical bottleneck: the reliance on the electricity grid. Widespread power outages pose a more immediate threat to national connectivity than direct physical damage to telecommunications towers or fiber lines. Furthermore, post-disaster recovery is complicated by logistical challenges; access to network sites for repairs can be severely hindered by damage to transport infrastructure [Source 7].

2.5 Digital Economy and Strategic Initiatives

The French government continues to invest in the digital sector through the "France 2030" plan, which aims to boost emerging technologies, digital security, and startups [Source 9]. Regulatory frameworks such as SecNumCloud are in place to ensure data security and sovereignty for cloud services operating within the nation [Source 9].

However, current intelligence does not identify specific government incentives designed to decentralize data center infrastructure outside of major metropolitan hubs. While major providers like Lumen Technologies and Zayo maintain fiber footprints and connectivity services that support the AI economy and international data transit, specific capacity figures for terrestrial fiber availability for cloud providers within France are not publicly detailed [Source 13, Source 14].

References

- [Source 1] Colocation and connectivity in global, AI-ready data centers - Equinix (https://www.equinix.com/data-centers)
- [Source 2] The State of 5G 2024 - GSMA Intelligence (https://gsmaintelligence.com/research/research-file-download?id=79791087&file=210224-The-State-of-5G-2024.pdf)
- [Source 3] 5G Observatory report 2025 - Shaping Europe's digital future (https://digital-strategy.ec.europa.eu/en/policies/5g-observatory-2025)
- [Source 4] New Peering Opportunities In The US And Europe For 2023 (https://www.consoleconnect.com/peering-opportunities-in-the-us-and-europe-for-2023/)
- [Source 5] Fixed Broadband and Superfast Broadband Market - Arcep (https://en.arcep.fr/news/press-releases/view/n/fixed-broadband-and-superfast-broadband-market-110925.html)
- [Source 6] Digital connectivity in France | Shaping Europe's digital future (https://digital-strategy.ec.europa.eu/en/policies/digital-connectivity-france)
- [Source 7] Enhancing the Resilience of Communication Networks | OECD (https://www.oecd.org/content/the-resilience-of-communication-networks_a47d78a1/d6920477-en.pdf)
- [Source 8] Bridging digital divides in G20 countries | OECD (https://www.oecd.org/content/dam/oecd/en digital-divides-in-g20-countries_daf5c059/35c1d850-en.pdf)
- [Source 9] France - Digital Economy - International Trade Administration (https://www.trade.gov/country commercial-guides/france-digital-economy)
- [Source 10] Wi-Fi & LoRaWAN® Deployment Synergies - LoRa Alliance (https://lora-alliance.org/wp-content/uploads/2020/11/wi-fi-and-lorawanr-deployment-synergies.pdf)
- [Source 11] U.S. vs. European Broadband Deployment: What Do the Data Say? (https://www.law.upenn.edu/live/files/3352-us-vs-european-broadband-deployment)
- [Source 12] Internet Exchange Points - Euro-IX (https://www.euro-ix.net/media/filer_public/cf/7c/cf7c8 40c9-4e37-9d79-02b61ccc081e/ixp_report_2020_.pdf)
- [Source 13] Lumen Technologies: AI-Ready Networking & Secure Cloud Solutions (https://www.lumen.com/en-us/home.html)
- [Source 14] Zayo: International Network Connectivity Services & Fiber Solutions

(https://www.zayo.com/)

Chapter 3

Market

Executive Summary

The French telecommunications market is a mature, highly competitive oligopoly characterized by intense price pressure and a high degree of market concentration. The sector is dominated by four primary mobile network operators (MNOs): Orange, SFR (Altice), Bouygues Telecom, and Free Mobile (Iliad Group) [Source 1]. Despite the stability of these four pillars, the market is currently undergoing a period of strategic turbulence driven by potential consolidation. Iliad Group has explicitly signaled intentions to strengthen its domestic position, shifting focus from international expansion to potential acquisitions within France, specifically targeting assets from the debt-laden Altice Group (SFR) [Source 2].

Financially, the market is defined by low Average Revenue Per User (ARPU), a long-term consequence of the aggressive pricing models introduced by Free Mobile in 2012. Operators face a "price war" environment where inflation erodes revenue growth, and service differentiation remains low [Source 3]. Despite these economic constraints, infrastructure performance remains robust. France ranks within the top 20 countries globally for mobile speeds, with Orange maintaining a leadership position in network quality and 5G consistency [Source 4, Source 5]. The market is currently driven by data consumption and service bundling rather than new disruptive entrants [Source 6].

3.1 Market Structure and Competitive Landscape

The French mobile market is structured around four major operators: Orange, SFR, Bouygues Telecom, and Free Mobile. Orange retains its status as the dominant player across all sectors, leveraging its historical position and extensive infrastructure [Source 1]. As of mid-2025, the market remains heavily concentrated. Bouygues Telecom reported a customer base of 27.1 million, while Free Mobile (Iliad) accounted for 23.1 million subscribers [Source 7].

The competitive dynamic is currently shifting towards consolidation. Iliad Group has ceased discussions regarding mergers in Italy to prioritize the French domestic market. This strategic

pivot is highlighted by a joint non-binding offer submitted by Bouygues Telecom, Free Mobile, and Orange to acquire significant portions of Altice's (SFR) activities [Source 8]. This move suggests a potential contraction of the market from four to three major network operators, driven by the financial instability of Altice and the desire of competitors to absorb SFR's market share and assets [Source 2].

3.2 Financial Dynamics and ARPU Trends

The economic environment for French mobile operators is challenging, characterized by low and declining ARPU. The market exhibits symptoms of a prolonged price war, where aggressive pricing strategies—originally instigated by Free Mobile's market entry—have become the norm. Growth in revenue per user is largely negated by inflation, and operators struggle to differentiate their services sufficiently to command premium pricing [Source 3].

Unlike markets where 5G adoption drives immediate revenue uplifts, the primary drivers for ARPU in France remain data consumption volume and the availability of service bundles [Source 6]. The market has not seen a new "disruptor" recently; rather, it continues to operate under the structural impact of the 2012 disruption caused by Free Mobile, which permanently altered consumer price expectations [Source 9].

3.3 Infrastructure and Network Performance

France maintains a high standard of mobile network performance, ranking within the top 20 nations globally for median mobile download speeds [Source 4]. Recent data indicates a median mobile download speed of approximately 50.48 Mbps and an upload speed of 13.08 Mbps [Source 10].

Network quality varies significantly by operator and region. Orange consistently outperforms competitors, recording the fastest speeds across all technologies, the highest 5G consistency, and the best gaming experience [Source 5]. Regional disparities are evident, with the Île-de-France region (Paris) recording median download speeds of 130.63 Mbps, nearly double that of Lower Normandy (72.34 Mbps) [Source 5]. This infrastructure leadership by Orange serves as a critical retention tool in a market otherwise defined by commoditized pricing.

References

- [Source 1] France Telecoms Market Report 2024, Featuring Orange, Iliad (https://uk.finance.yahoo.com/n telecoms-market-report-2024-082700071.html)
- [Source 2] France's Iliad drops Italian tie-up plan; Telecom Italia shares fall (https://www.reuters.com/en/frances-iliad-drops-italian-tie-up-plan-telecom-italia-shares-fall-2025-08-28/)
- [Source 3] The state of competition in telecoms - PwC (https://www.pwc.com/gx/en/industries/tmt/telec state-of-competition.html)

- [Source 4] Speedtest Global Index Market Analyses Now Available for 43 … (https://www.ookla.com/articl index-market-analyses-q1-2022)
- [Source 5] Speedtest® Connectivity Report | France H1 2024 - Ookla (https://www.ookla.com/research/re speedtest-connectivity-report-h12024)
- [Source 6] THE EVOLUTION OF DATA GROWTH IN EUROPE - Arthur D. Little (https://www.adlittle.com/sites/default/files/reports/ADL_Data_growth_Europe_2023.pdf)
- [Source 7] Bouygues Telecom, Free-iliad Group and Orange joint statement … (https://newsroom.orange.com/bouygues-telecom-free-iliad-group-and-orange-joint-statement-following-the-rejection-of-their-acquisition-bid-by-altice-france/)
- [Source 8] Bouygues Telecom, Free-iliad Group and Orange submit a joint non … (https://newsroom.orange.com/bouygues-telecom-free-iliad-group-and-orange-submit-a-joint-non-binding-offer-to-acquire-a-large-part-of-altices-activities-in-france/)
- [Source 9] An analysis of the disruptive impact of the entry of Free Mobile … - HAL (https://hal.science/hal-02147914/document)
- [Source 10] Speedtest Global Index – Internet Speed around the world (https://www.speedtest.net/global-index)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 4

Localization

Executive Summary

France's localization strategy is defined by a tension between a high reliance on U.S. hyperscalers for critical infrastructure and an aggressive government-led push for "digital sovereignty." While global providers like AWS, Azure, and Google Cloud dominate the French enterprise and public sector market due to superior service portfolios and R&D capabilities [Source 12], the French government has implemented a rigorous regulatory framework to counter extraterritorial legal risks. This includes the "Cloud de Confiance" (Trusted Cloud) doctrine, which mandates SecNumCloud certification for sensitive data and encourages partnerships where U.S. technology is licensed to European entities to mitigate the reach of the U.S. CLOUD Act [Source 1].

The "France 2030" investment plan allocates significant capital—including €667 million for cloud computing and over €100 million for AI infrastructure—to foster domestic champions like Mistral AI and Scaleway [Source 2, Source 3]. However, legal jurisdiction remains a primary threat; the French Data Protection Agency (CNIL) continues to flag the incompatibility of U.S. surveillance laws (FISA 702) with GDPR, challenging the viability of transferring sensitive data, such as health records, to foreign-hosted clouds [Source 9]. Despite these challenges, France maintains a robust national internet ecosystem, characterized by strong trust in the .fr ccTLD and active management of local internet exchange points [Source 10, Source 11].

4.1 Sovereign Cloud Infrastructure and Market Dynamics

The French cloud market is characterized by a significant disparity between domestic capabilities and the dominance of U.S. hyperscalers. Global providers (AWS, Azure, Google Cloud) hold a commanding market share in the enterprise and public sectors. This dominance is driven by a "Service Portfolio Canyon," where hyperscalers offer over 200 services compared to the 15–60 services typically offered by European providers, alongside a massive R&D spending gap ($150 billion for U.S. giants versus €500 million for the European industry) [Source 6].

To address this, the French government has deployed a "Cloud First" policy for public digital

projects, requiring that sensitive data be hosted on government clouds or commercial services possessing **SecNumCloud** certification [Source 3]. This certification, managed by the national cybersecurity agency (ANSSI), is the cornerstone of the "Cloud de Confiance" strategy. This strategy acknowledges the technical superiority of U.S. providers but attempts to insulate data from extraterritorial laws by encouraging joint ventures where U.S. software is operated by French entities [Source 1].

Under the "France 2030" plan, the government is actively financing the reduction of reliance on foreign infrastructure. Key initiatives include: * **Cloud Acceleration:** A €667 million allocation to support the cloud computing ecosystem [Source 3]. * **AI Infrastructure:** Partnerships with NVIDIA to build supercomputing capacity for French AI startups like Mistral AI, and the expansion of Scaleway's GPU offerings to ensure domestic AI processing capabilities [Source 2]. * **Quantum Computing:** Investment in Quandela, the first EU company to make quantum computers accessible via the cloud, hosted in OVHcloud datacenters [Source 4].

4.2 Legal Jurisdiction and Extraterritorial Risks

The primary driver of France's localization policy is the legal risk posed by the extraterritorial reach of non-EU laws, specifically the U.S. CLOUD Act. This legislation allows U.S. authorities to compel service providers to disclose data regardless of where it is physically stored, creating a direct conflict with EU frameworks like GDPR and the NIS2 Directive [Source 7].

The French Data Protection Agency (CNIL) has identified significant risks regarding data residency: * **Surveillance Incompatibility:** The CNIL views U.S. surveillance laws, particularly Section 702 of FISA and Executive Order 12333, as incompatible with EU privacy rights. This has led to strict interpretations of the *Schrems II* ruling, casting doubt on the legality of transferring personal data to U.S. providers even when Standard Contractual Clauses (SCCs) are used [Source 9]. * **Health Data Hub:** The CNIL has specifically recommended against hosting the national Health Data Hub on Microsoft Azure due to the risk of access by U.S. intelligence services, highlighting that corporate structure alone cannot guarantee immunity from foreign legal demands [Source 8, Source 9]. * **Sovereignty Definition:** French strategic analysis increasingly defines sovereignty not merely by the physical location of servers (data residency), but by the immunity of that data from foreign jurisdiction. Consequently, "sovereign cloud" initiatives are judged by their ability to legally shield data from the U.S. CLOUD Act [Source 8].

4.3 Network Localization and Digital Identity

France maintains a strong preference for national network assets, though specific data on traffic routing remains opaque. While the exact percentage of internet traffic exchanged locally versus "tromboned" through international points is not publicly quantified, the ecosystem is supported by France-IX, which facilitates local peering [Source 13].

In the domain name sector, there is a distinct preference for localized digital identity: * **ccTLD Dominance:** European markets, including France, show a 58% market share preference for national country code Top-Level Domains (ccTLDs) over generic domains. The .fr domain is managed by Afnic, a central player in the French digital infrastructure [Source 11]. * **Brand TLDs:** There is high acceptance of "dot brand" TLDs in France, with 83% of respondents in perception surveys acknowledging that such domains aid in immediate business identification [Source 10].

While France is integrating with the upcoming European Digital Identity Wallet (EUDIW) scheduled for 2026, specific adoption rates for purely domestic digital identity solutions for public service access remain undocumented in open sources [Source 14].

References

- [Source 1] France - Digital Economy - International Trade Administration (https://www.trade.gov/country commercial-guides/france-digital-economy)
- [Source 2] France Bolsters National AI Strategy With NVIDIA Infrastructure (https://blogs.nvidia.com/blog/france-sovereign-ai-infrastructure/)
- [Source 3] French strategy for cloud computing & data sharing - Gaia-X (https://gaia-x.eu/wp-content/uploads/2023/03/03.15-10.30-Adrien-Laroche-French-strategy-cloud-and-data-1.pdf)
- [Source 4] Quandela secures €50 million to support international expansion (https://www.quandela.com/a us/newsroom/quandela-secures-e50-million-to-support-international-expansion/)
- [Source 5] MAKE FRANCE AN AI POWERHOUSE (https://www.elysee.fr/admin/upload/default/0001
- [Source 6] European Cloud Reality Check: Why Your Local Heroes Can't… (https://www.linkedin.com/pu cloud-reality-check-why-your-local-heroes-cant-hermann-skboe)
- [Source 7] The CLOUD Act and Transatlantic Trust - CSIS (https://www.csis.org/analysis/cloud-act-and-transatlantic-trust)
- [Source 8] Theodore Christakis' Post - LinkedIn (https://www.linkedin.com/posts/theodore-christakis-9ab5a6260_episode-0221-canadian-court-european-data-activity-7401160641425678342-ELjM)
- [Source 9] Transfers of Health Data from France to the United States Not… (https://www.mwe.com/insights/transfers-of-health-data-from-france-to-the-us-are-not-prohibited-by-the-french-data-protection-authority-or-french-courts/)
- [Source 10] "Dot brand" TLDs: Afnic reveals the exclusive results of its… (https://www.afnic.fr/en/observa and-resources/expert-papers/dot-brand-tlds-afnic-reveals-the-exclusive-results-of-its-perception-survey/)
- [Source 11] 2023 | The European domain market - Snapshot Hub by InterNetX (https://snapshot.internetx.com/en/the-european-domain-market-in-2023/)
- [Source 12] Top Cloud Providers in 2024 - Hyperscalers and Alternative vendors (https://holori.com/top-cloud-providers-in-2024/)
- [Source 13] Enhance your company's Internet connectivity with our multi… (https://www.franceix.net/en/

- [Source 14] The State of Digital Identity in Europe 2024 – 2025 (https://5310879.fs1.hubspotusercontent-na1.net/hubfs/5310879/The-State-of-Digital-Identity-in-Europe-report-2024-2025-Signicat.pdf)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 5

Security

Executive Summary

France exhibits a highly mature posture in network routing security, characterized by an exceptionally high implementation rate of Resource Public Key Infrastructure (RPKI) across its Autonomous Systems. Current intelligence places France 14th on the National Cyber Security Index (NCSI), reflecting a strong national framework for cyber defense [Source 1]. Despite these strengths, significant intelligence gaps remain regarding specific adoption rates for Mutually Agreed Norms for Routing Security (MANRS) and current granular metrics for DNSSEC validation. While the topological structure of the French internet relies heavily on specific critical nodes, such as Cogent and Orange, the high RPKI coverage mitigates some risks associated with route hijacking. Conversely, specific data regarding current malware infection rates and DDoS attack volumes targeting French infrastructure remains insufficient for a definitive threat assessment.

5.1 Network Infrastructure and Routing Security

France has achieved a leading position in routing security protocols. Internal network analysis indicates that 98.55% of French Autonomous System Numbers (ASNs) have implemented RPKI for their announced prefixes [IYP-GRAPH]. This high level of cryptographic verification significantly reduces the attack surface for Border Gateway Protocol (BGP) hijacking and route leaks.

Despite this high technical validation rate, the broader adoption of industry-standard cooperative frameworks remains difficult to quantify. Intelligence regarding the specific number of French Internet Service Providers (ISPs) compliant with MANRS is currently inconclusive, as major ecosystem analyses do not provide country-level breakdowns [Source 2]. While major providers like Orange Wholesale International offer IP Transit services to ISPs, their specific compliance status or that of their downstream clients is not publicly detailed [Source 3].

5.2 Critical Topological Chokepoints

The resilience of the French internet architecture is heavily dependent on a select group of major ASNs that serve as critical chokepoints. Analysis of incoming dependency relationships (`DEPENDS_ON`) highlights COGENT-174 as the most significant node, with 199,965 incoming dependencies. This is followed by Opentransit Orange S.A. (29,376 dependencies) and COLT Technology Services Group Limited (9,290 dependencies) [IYP-GRAPH].

Other significant infrastructure providers include F5 Networks SARL and Zayo Infrastructure France SA. The concentration of routing dependencies on these specific entities indicates that while RPKI coverage is high, the physical and logical availability of these specific networks is paramount to national connectivity.

5.3 Cyber Governance and Threat Landscape

France's strategic commitment to cybersecurity is reflected in its global standing, currently ranking 14th on the National Cyber Security Index (NCSI) [Source 1]. This index evaluates the implementation of cyber legislation and national cyber units.

However, the current operational threat landscape presents visibility challenges. Intelligence regarding the specific volume of Distributed Denial of Service (DDoS) attacks and the rate of malware infections targeting France is currently limited. While historical data points to significant incidents such as the WannaCry ransomware attack and breaches in the retail sector, current, definitive statistics on botnet activity originating from or targeting France are unavailable [Source 4]. Similarly, while global reports track malware families like Phorpiex and Emotet, they do not currently offer a specific breakdown for French infection rates [Source 5].

Furthermore, data regarding the validation of Domain Name System Security Extensions (DNSSEC) is fragmented. While total DNS queries originating from France have been observed (36,473 in sample data), the proportion resolved by validating resolvers remains unquantified in current technical findings [IYP-GRAPH].

References

- [Source 1] NCSI :: Ranking - National Cyber Security Index (https://ncsi.ega.ee/ncsi-index/)
- [Source 2] Mind Your MANRS: Measuring the MANRS Ecosystem - CAIDA (https://www.caida.org/catalog/papers/2022_mind_your_manrs/mind_your_manrs.pdf)
- [Source 3] IP Transit for global connectivity | Orange Wholesale International (https://wholesale.orange.com/international/en/our-solutions/ip-transit.html)
- [Source 4] Cybersecurity Threat Landscape in France - Kiteworks (https://www.kiteworks.com/cybersecu risk-management/threat-landscape-in-france/)
- [Source 5] November 2020's Most Wanted Malware: Notorious Phorpiex Botnet …

(https://www.checkpoint.com/press-releases/november-2020s-most-wanted-malware-notorious-phorpiex-botnet-returns-as-most-impactful-infection/)

- [IYP-GRAPH] Internal Knowledge Graph (Internal Intelligence Data)

Chapter 6

Governance

Executive Summary

France maintains a sophisticated governance framework for the digital and telecommunications sectors, characterized by a "Brussels Model" approach that emphasizes strict regulation, alignment with European Union (EU) standards, and the protection of fundamental rights [Source 1 - Policy Review]. Unlike state-controlled models, French governance operates within a liberal democratic context where regulatory powers are balanced against judicial oversight and civil liberties. The nation has fully integrated the General Data Protection Regulation (GDPR) and enforces strict Net Neutrality rules under the oversight of the Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) and the Commission Nationale de l'Informatique et des Libertés (CNIL) [Source 1 - Kiteworks][Source 2 - Arcep].

While the state retains significant capabilities for national security surveillance, these powers are constrained by Court of Justice of the European Union (CJEU) rulings which prohibit general and indiscriminate data retention absent a genuine and present threat [Source 1 - Jones Day]. Strategically, France is positioning itself as a leader in ethical technology through its 2018 "AI for Humanity" strategy and active participation in international cybercrime frameworks, including the Budapest Convention [Source 2 - AI Watch][Source 2 - CoE].

6.1 Regulatory Framework and Institutional Oversight

The French telecommunications and digital landscape is governed by the *Code des postes et des communications électroniques* (CPCE), which transposes the EU Electronic Communications Code into national law. The licensing and authorization of operators are managed by ARCEP, an independent administrative authority [Source 3 - ICLG].

Regulatory Independence and Enforcement ARCEP operates within a framework heavily influenced by EU regulations. Its powers were significantly expanded by the Law No. 2016-1321 of 7 October 2016 for a Digital Republic, which granted new investigatory and sanctioning

capabilities [Source 1 - Latham & Watkins]. Unlike regulators in less developed jurisdictions, ARCEP possesses the capacity to enforce regulations effectively against incumbent operators, ensuring a competitive market structure [Source 4 - World Bank]. However, the regulator's powers are subject to constitutional checks; the *Conseil constitutionnel* has previously intervened to redact legislation deemed unconstitutional, such as provisions within online hate speech laws, demonstrating a functional system of checks and balances [Source 3 - ICLG].

Data Protection Governance France enforces a rigorous data protection regime aligned with the GDPR. The CNIL serves as the primary enforcement body, wielding supervisory and investigative powers to issue warnings, compliance orders, and fines against both corporate and state entities [Source 1 - Kiteworks]. This framework ensures that data processing adheres to principles of consent, minimization, and security [Source 3 - White & Case].

6.2 Surveillance, Privacy, and Civil Liberties

French governance in the digital domain is defined by a continuous tension between national security imperatives and the protection of privacy rights.

Surveillance Limitations French law regarding state surveillance is subject to EU legal scrutiny. The CJEU has ruled that French legislation requiring Electronic Communications Service (ECS) providers to retain traffic and location data on a general and indiscriminate basis is contrary to EU law [Source 1 - Jones Day]. Surveillance measures are only permissible under a "serious threat" to national security that is genuine and foreseeable. Any retention of data must be proportionate, limited in duration, and subject to clear rules and minimum safeguards to prevent arbitrary abuse [Source 1 - Jones Day][Source 2 - Atlantic Council].

Net Neutrality and Censorship France strictly adheres to the EU Open Internet Regulation (Regulation (EU) 2015/2120). ISPs are legally prohibited from blocking, throttling, or engaging in paid prioritization of traffic [Source 2 - Arcep]. ARCEP actively monitors compliance to ensure the internet remains open and non-discriminatory [Source 3 - La Quadrature]. Regarding censorship, there is no evidence of government-mandated internet shutdowns or widespread social media blocking in France in recent years [Source 1 - Brookings]. While legislation exists to block specific illicit content (e.g., child abuse images, terrorism), these measures are targeted and subject to significant political and legal debate regarding their effectiveness and impact on civil liberties [Source 1 - Policy Review][Source 3 - USENIX].

6.3 Strategic Digital Policy and International Cooperation

The French government pursues a proactive strategy to shape the digital environment domestically and globally, moving beyond simple regulation toward active ecosystem development.

National AI Strategy The cornerstone of recent policy is the "AI for Humanity" strategy launched in 2018. This initiative aims to foster an ethical AI ecosystem by focusing on education, open data policies, research innovation, and the development of high-performance computing

infrastructure [Source 2 - AI Watch]. The objective is to bridge the skills gap and position France as a global leader in ethical AI development.

International Cyber Governance France is a party to the Budapest Convention on Cybercrime, which harmonizes national laws on cyber-offenses and facilitates international cooperation on electronic evidence [Source 2 - CoE]. Beyond this, France supports the development of new international instruments, such as the UN Convention against Cybercrime, provided they include safeguards against abuse by authoritarian regimes [Source 2 - Diplomatie.gouv]. France's international digital strategy emphasizes capacity building, cyber resilience, and the promotion of a secure, open, and inclusive digital world [Source 1 - Expertise France][Source 4 - Diplomatie.gouv].

References

- [Source 1 - Jones Day] End of the EU's Data Retention Saga? - Jones Day (https://www.jonesday.com/en/insights/2020/10/cjeu-clarifies-conditions-for-state-surveillance-regimes)
- [Source 1 - Latham & Watkins] Technology, Media and Telecommunications Review (https://www.lw.com/en/insights/2018/01/technology-media-telecommunications-review-2018-France)
- [Source 1 - Kiteworks] French Data Protection Act: Protecting Data Privacy in France (https://www.kiteworks.com/risk-compliance-glossary/french-data-protection-act/)
- [Source 1 - Brookings] Internet shutdowns cost countries $2.4 billion last year (https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf)
- [Source 1 - Policy Review] Internet filtering trends in liberal democracies: French and German regulatory debates (https://policyreview.info/articles/analysis/internet-filtering-trends-liberal-democracies-french-and-german-regulatory-debates)
- [Source 1 - Expertise France] Our work in digital inclusion and accessibility - Expertise France (https://www.expertisefrance.fr/en/expertise/digital-inclusion-and-accessibility)
- [Source 2 - Atlantic Council] Putting privacy limits on national security mass surveillance (https://www.atlanticcouncil.org/blogs/new-atlanticist/putting-privacy-limits-on-national-security-mass-surveillance-the-european-court-of-justice-intervenes/)
- [Source 2 - CoE] Cybercrime … - https: //rm. coe. int (https://rm.coe.int/cyber-rp-breakfast-nov2024-final/1680b28562)
- [Source 2 - AI Watch] France AI Strategy Report - AI Watch - European Commission (https://ai-watch.ec.europa.eu/countries/france/france-ai-strategy-report_en)
- [Source 2 - Diplomatie.gouv] France's international action to fight cyber crime (9 Jan. 2025) (https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/france-s-international-action-to-fight-cyber-crime-9-jan-2025)
- [Source 2 - Arcep] Net neutrality - Arcep (https://en.arcep.fr/uploads/tx_gspublication/RA-2023-TOME3-ENG-net-neutrality_july2023.pdf)
- [Source 3 - Arcep] Arcep in Europe and around the world (https://en.arcep.fr/arcep/arcep-

europe-international.html)
- [Source 3 - White & Case] GDPR Guide to National Implementation: France - White & Case LLP (https://www.whitecase.com/insight-our-thinking/gdpr-guide-national-implementation-france)
- [Source 3 - USENIX] Internet Filtering Trends in Western Liberal Democracies - USENIX (https://www.usenix.org/system/files/conference/foci12/breindl2012foci.pdf)
- [Source 3 - La Quadrature] Net Neutrality: France Is Playing The Telcos' Game (https://www.laquadrature.net/en/2014/12/03/net-neutrality-france-is-playing-the-telcos-game/)
- [Source 3 - ICLG] Telecoms, Media and Internet Laws and Regulations France 2026 (https://iclg.com/practice-areas/telecoms-media-and-internet-laws-and-regulations/france)
- [Source 4 - World Bank] Chad - The World Bank (https://thedocs.worldbank.org/en/doc/61714f214ed04b
0400012021/related/Chad-country-diagnostic.pdf)
- [Source 4 - Diplomatie.gouv] France and Cyber security - Ministry for Europe and Foreign Affairs (https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/)

Chapter 7

Strategic Synthesis & Roadmap

Chapter 8

Section 7: Strategic Synthesis & Roadmap

Role: Chief Strategy Officer to the Head of State. **Date:** October 2025 **Subject:** The "Sovereign Soil, Foreign Routing" Paradox – Strategic Recommendations.

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

The Narrative: France stands as a global paradox in the digital domain. We possess a "Ferrari" of physical infrastructure—leading the world in fiber deployment (FTTH) and routing security (RPKI)—yet the engine driving our traffic is imported. We have successfully asserted **Regulatory Sovereignty** through the CNIL and ANSSI, creating a legal fortress against foreign interference. However, we have failed to achieve **Logical Sovereignty**.

The Paradox: "Sovereign Soil, Foreign Routing." While our laws (GDPR, SecNumCloud) are strictly French/European, our actual data transit is dangerously dependent on a single US entity: Cogent Communications (AS174). Our intelligence reveals a massive upstream dependency where French networks, including critical research and telecom infrastructure, rely disproportionately on this foreign Tier 1 provider. Furthermore, while we fund "sovereign AI" and cloud initiatives, the "Service Portfolio Canyon" forces our enterprises to rely on US Hyperscalers (AWS, Azure) for functionality, exposing us to the US CLOUD Act.

The Diagnosis: France is digitally secure against cyber-criminals (high RPKI), but strategically vulnerable to geopolitical coercion (Cogent dependency and US Cloud dominance).

8.2 2. SWOT Analysis: The Strategic Cheat Sheet

STRENGTHS (Internal Assets)	WEAKNESSES (Internal Flaws)
Physical Layer Dominance: 79% Fiber penetration and global leadership in subsea cables (Alcatel Submarine Networks).	**The Cogent Chokepoint:** Critical over-reliance on AS174 for upstream transit creates a single point of geopolitical failure.
Cyber Hygiene: World-leading RPKI adoption (98.55%) makes the French routing ecosystem highly resistant to hijacking.	**Market Fragility:** A brutal price war has left operators (specifically SFR/Altice) debt-laden, limiting their capacity for R&D investment.
Regulatory Muscle: ANSSI and CNIL provide the world's most robust framework for data protection and state surveillance oversight.	**Grid Dependency:** Telecommunications resilience is tethered to the power grid; power outages (Storm Ciaran) immediately kill connectivity.

OPPORTUNITIES (External Trends)	THREATS (External Dangers)
The "Marseille Gateway": Position France as the primary digital bridge between Europe and Africa/Middle East via subsea cables.	**Extraterritorial Law:** The US CLOUD Act renders "data residency" insufficient; French data on US clouds is legally exposed.
AI Sovereignty: Leverage "France 2030" to turn Mistral AI and Scaleway into a viable "third way" alternative to US/Chinese tech.	**Distressed Asset Acquisition:** The potential collapse of Altice (SFR) risks critical infrastructure being sold to non-aligned foreign capital.
Post-Quantum Cryptography: Lead the EU in upgrading the already secure RPKI framework to quantum-resistant standards.	**The "Service Canyon":** If domestic clouds cannot match Hyperscaler features, French industry will ignore sovereignty mandates for efficiency.

8.3 3. Strategic Roadmap: The Policy Agenda

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

Focus: Securing the Perimeter and Breaking Chokepoints.

- **Directive 1: The "Multi-Homing" Mandate.**
  - **Action:** Issue a decree requiring all Operators of Vital Importance (OIV) and critical public infrastructure (RENATER) to demonstrate upstream diversity.
  - **Goal:** Reduce the dependency on Cogent (AS174) by mandating a secondary, non-US Tier 1 transit provider (e.g., Telia, Deutsche Telekom) for all critical state traffic.
- **Directive 2: Energy Resilience Audit.**

  - **Action:** In response to Storm Ciaran findings, mandate a 72-hour independent power backup (batteries/generators) for all mobile towers in designated "strategic zones."
  - **Goal:** Decouple telecommunications availability from immediate grid fluctuations.
- **Directive 3: Distressed Asset Shield.**
  - **Action:** Pre-authorize the *Fonds Stratégique d'Investissement* (FSI) to intervene in the potential sale of SFR/Altice assets.
  - **Goal:** Prevent critical mobile infrastructure from falling under non-EU ownership during the inevitable market consolidation.

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

Focus: Closing the Industrial Gap.

- **Initiative: The "Cloud Feature" Subsidy.**
  - **Action:** Shift "France 2030" funding from general R&D to specific feature parity. Subsidize domestic cloud providers (OVH, Scaleway) specifically to build the "missing 150 services" (PaaS, Serverless) that currently force French companies to Azure/AWS.
  - **Goal:** Make the "Cloud de Confiance" commercially viable, not just legally compliant.
- **Initiative: The Marseille-Africa Digital Corridor.**
  - **Action:** Incentivize the landing of new subsea cables in Marseille and Bordeaux, specifically those bypassing US/UK control points.
  - **Goal:** Cement France as the indispensable data hub for the Global South, leveraging Alcatel's industrial capacity.

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

Focus: True Autonomy.

- **Vision: Sovereign AI Stack.**
  - **Action:** Build a fully sovereign AI value chain: French Chips (STMicro) + French Cloud (Scaleway) + French Models (Mistral) + French Data (Public Sector).
  - **Goal:** Ensure the French state can operate AI governance tools without relying on NVIDIA hardware or OpenAI APIs.
- **Vision: The "Brussels-Paris" Standard.**
  - **Action:** Export the SecNumCloud standard to the entire EU, making it the *de facto* requirement for the European Single Market.
  - **Goal:** Create a market size large enough to sustain European cloud providers against US giants.

8.4 4. Final Verdict

8.4.1 Investability Score: HIGH

France offers a unique proposition: it is the safest "bunker" in the digital world. The combination of nuclear energy stability, high fiber penetration, and the world's strictest routing security (RPKI) makes it the ideal location for high-value data storage and processing. The regulatory environment is strict but predictable.

8.4.2 Maturity Score: MATURE (with Structural Risks)

The market is fully developed with 5G and Fiber ubiquity. However, it is financially stressed (low ARPU) and topologically unbalanced (Cogent dependency). We are a "Mature" digital nation that has outsourced its "Logical" nervous system. The next 5 years must be spent repatriating that control.