STRATEGIC COUNTRY REPORT: FINLAND

Automated Strategic Analyst (v2.2 Parallel)

12 February 2026

Contents

Chapter 1

Geopolitics

Executive Summary

Finland's geopolitical posture is increasingly defined by its dual role as a digitally advanced nation and a frontline state in the emerging domain of seabed warfare. The nation's strategic stability is heavily contingent upon the security of submarine infrastructure in the Baltic Sea, a vulnerability exposed by recent sabotage incidents involving the *Balticconnector* and *C-Lion1* cables [Source 1][Source 3]. While Finland actively champions digital sovereignty through European Union (EU) frameworks and Nordic cooperation, technical analysis reveals significant reliance on external digital entities. Specifically, the network topology exhibits a high degree of centralization, with Cloudflare identified as a critical dependency for global connectivity [Internal Graph]. Consequently, Finland's geopolitical strategy has pivoted toward fortifying physical infrastructure resilience and deepening integration with Western digital alliances to mitigate the risks of hybrid warfare and foreign coercion [Source 2][Source 4].

1.1 Strategic Vulnerability of Submarine Infrastructure

Finland's geographical position renders it effectively an "island" regarding digital and energy connectivity, relying heavily on submarine cables traversing the Baltic Sea. This dependence has transformed the maritime domain into a primary theater for hybrid threats. Intelligence indicates that Finland is a direct target of seabed interference; specifically, the severing of the *C-Lion1* and *BCS East-West Interlink* cables in November 2024, and the damage to the *Balticconnector* pipeline and data cables in October 2023 [Source 1][Source 3].

These incidents, linked to vessels subsequently tracking toward Russian Arctic waters, highlight the fragility of Finland's physical link to the European mainland [Source 3]. While the immediate operational impact was mitigated by European redundancy, the geopolitical implication is clear: hostile actors possess the capability and intent to disrupt Finland's critical connectivity. Unlike a transit hub for landlocked nations—Finland's neighbors Russia and Norway possess their own coastlines—Finland functions as a terminal node in the Baltic rim network. The security of these cables is not merely a commercial concern but a matter of national sovereignty, necessitating enhanced seabed surveillance and cooperation with NATO and Nordic partners [Source 1].

1.2 Digital Sovereignty and Network Topology Risks

Despite Finland's political advocacy for digital sovereignty and the EU Digital Single Market, technical network analysis exposes acute structural vulnerabilities. Finland's internet architecture is characterized by significant centralization. Intelligence reveals that **Cloudflare (ASN 13335)** acts as a massive chokepoint, holding 956 incoming dependencies from other networks [Internal Graph]. This is followed by **GlobalConnect (ASN 12552)** with 747 dependencies [Internal Graph]. This concentration creates a "single point of failure" risk; a targeted outage or compromise of these specific Tier 1/Tier 2 providers could catastrophically sever Finland's global digital reach.

Furthermore, the resilience of Finland's routing infrastructure against hijacking attacks is moderate. The adoption of Resource Public Key Infrastructure (RPKI)—a security standard to validate route origins—stands at approximately **56.32%** [Internal Graph]. While this indicates progress, nearly half of the country's routing infrastructure remains vulnerable to route leaks or malicious redirection, a vector often exploited by state-sponsored actors to intercept data traffic.

1.3 International Alliances and Connectivity Strategy

To counterbalance these physical and technical vulnerabilities, Finland has integrated its digital strategy deeply with Western alliances. Finland is a key participant in the **EU-Latin America and Caribbean (EU-LAC) Digital Alliance**, leveraging this partnership to promote a human-centric digital model and export its expertise in 5G and cybersecurity [Source 5][Source 8]. This participation aligns with the EU's Global Gateway Strategy, allowing Finland to project influence and shape global digital governance standards alongside democratic allies [Source 5].

Regionally, Finland relies on international Internet Exchange Points (IXPs) for traffic exchange. Analysis of peering data indicates that with the exception of the national *PITER-IX Helsinki*, Finland's incumbent operators peer predominantly at international exchange points [Internal Graph]. This reliance on cross-border traffic exchange reinforces the necessity of the "Digital North" strategy, where Nordic nations are urged to treat digital infrastructure as a shared security asset, pooling resources for backup systems to prevent a regional digital blackout [Source 2].

References

- [Source 1] Recorded Future: Submarine Cable Security at Risk Amid Geopolitical Tensions (https://www.recordedfuture.com/research/submarine-cables-face-increasing-threats)

- [Source 2] The Nordics must strengthen their digital preparedness to avoid a digital blackout (https://www.mynewsdesk.com/globalconnect/pressreleases/new-whitepapers-the-nordics-must-strengthen-their-digital-preparedness-to-avoid-a-digital-blackout-3414680)
- [Source 3] Wilson Center: Seabed Warfare Against Data Cables (https://www.wilsoncenter.org/sites/defau
  Warfare-Cables%20%281%29.pdf)
- [Source 4] Defending the North Amid Rising Geopolitical Tensions - CSIS (https://www.csis.org/analysis/
  north-amid-rising-geopolitical-tensions)
- [Source 5] EU-Latin America and Caribbean Digital Alliance (https://international-partnerships.ec.europa.eu/policies/global-gateway/eu-latin-america-and-caribbean-digital-alliance_en)
- [Source 6] What is digital sovereignty and how are countries approaching it? (https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/)
- [Source 7] Finland 2024 Digital Decade Country Report (https://digital-strategy.ec.europa.eu/en/factpage
  2024-digital-decade-country-report)
- [Source 8] Finland’s Contributions to NATO: Strengthening the Alliance’s Nordic and Arctic Fronts (https://www.wilsoncenter.org/article/finlands-contributions-nato-strengthening-alliances-nordic-and-arctic-fronts)
- [Internal Graph] IYP-GRAPH: Internal Network Topology and ASN Data Analysis

Chapter 2

Infrastructure

Executive Summary

Finland possesses a highly advanced, albeit geographically bifurcated, digital infrastructure characterized by near-ubiquitous mobile coverage and a strategic reliance on a consolidated group of domestic operators. As of mid-2024, Finland has achieved approximately 100% population coverage for 5G, with high-speed 5G available to 91% of households [Source 2]. However, significant disparities persist in fixed network infrastructure; while urban centers benefit from high fiber penetration, rural areas face a connectivity gap, with over half of households in sparsely populated regions lacking fast fixed connections [Source 4].

The national network topology is heavily centralized. Three major operators—Elisa Oyj, DNA Oyj, and Telia Finland—control over 80% of the Autonomous System Number (ASN) landscape [IYP-GRAPH]. While this consolidation facilitates rapid technology deployment, such as the 3.5 GHz 5G rollout, it creates critical dependencies. Analysis of interconnection points reveals that entities like GlobalConnect and Cloudflare serve as potential chokepoints due to high downstream dependencies [IYP-GRAPH]. Furthermore, the physical security of subsea infrastructure in the Baltic Sea remains a primary strategic concern due to geopolitical tensions and recent incidents of cable damage [Source 1]. Finland's resilience strategy is currently pivoting toward a "Hybrid Sovereign Model" for data centers and strict alignment with EU critical infrastructure directives to mitigate these physical and cyber vulnerabilities [Source 2].

2.1 Mobile and Fixed Network Architecture

Mobile Network Deployment and Spectrum Finland maintains a leading position in mobile network availability. By the end of June 2024, high-speed 4G or 5G networks covered 96% of households [Source 2]. The deployment of "invisible highways" for mobile traffic has been facilitated by the allocation of the 3.4–3.8 GHz spectrum band. In the most recent auction, the Finnish government secured €77.6 million, with licenses divided equally (130 MHz each) among the three incumbent operators: Telia Finland, Elisa Corp., and DNA Oy [Source 2].

Despite high aggregate statistics, “white spots” with poor or non-existent coverage persist. These gaps are driven by geographic challenges, including difficult terrain and sparse settlement patterns that reduce commercial incentives for infrastructure investment [Source 1][Source 2]. Operational anomalies have also been observed in border regions; near the Russian border, devices may inadvertently switch to Russian networks, while similar interference issues affect users near the Norwegian border [Source 2].

Fixed Broadband and Fiber Penetration Finland’s National Broadband Plan targets 1 Gbps access for all households by 2030. As of September 2024, 75% of households had access to 1 Gbps speeds, and the Fiber to the Home (FTTH) penetration rate stood at 68% [Source 4].

A sharp urban-rural divide characterizes the fixed network landscape. In urban areas, over 90% of households have access to 100 Mbps connections. In contrast, rural areas close to cities and sparsely populated regions lag significantly, with more than 50% of households lacking fast fixed connections [Source 4]. This disparity highlights the limitations of market-driven infrastructure deployment in low-density zones.

2.2 Internet Routing and Interconnection

Autonomous System Landscape The Finnish IP routing landscape is highly concentrated. The three primary operators account for the vast majority of the ASN market share: Elisa Oyj (32.68%), DNA Oyj (28.11%), and Telia Finland Oyj (20.93%) [IYP-GRAPH].

Critical Interconnection Nodes Inter-network connectivity relies heavily on specific physical and logical hubs. * **Physical Hubs:** EUNET-FINLAND (Elisa Oyj) and GlobalConnect (AS12552) are identified as critical physical interconnection hubs. Elisa maintains 3,918 direct peering relationships, while GlobalConnect maintains 3,540 [IYP-GRAPH]. * **Dependency Chokepoints:** GlobalConnect exhibits the highest incoming dependency count (747), indicating its role as a central node upon which numerous other networks rely. Additionally, Cloudflare (CLOUDFLARENET) shows a disproportionately high number of downstream dependencies (956), representing a potential logical bottleneck or single point of failure for hosted services [IYP-GRAPH].

Routing Security Current intelligence indicates a critical gap in routing security hygiene. The adoption rate for Resource Public Key Infrastructure (RPKI) among announced IP prefixes in Finland is reported at 0.0% [IYP-GRAPH]. This lack of cryptographic validation for BGP announcements increases the national network’s vulnerability to route hijacking and misconfiguration.

Internet Exchange Points (IXPs) The primary peering infrastructure is managed by the Finnish Communication and Internet Exchange (FICIX), which operates three nodes: FICIX-1 in Espoo (Otaniemi), FICIX-2 in Helsinki (Pasila), and FICIX-3 in Oulu [Source 3]. As of 2024, FICIX had 54 members, serving as the central clearinghouse for domestic traffic exchange [Source 3].

2.3 Data Center and Strategic Infrastructure

Sovereign Data Strategy Finland is advancing a “Hybrid Sovereign Model” for its data infrastructure. This strategic framework entails government ownership and operation of “core” data centers for critical and classified workloads, while partnering with the private sector for non-sensitive data [Source 2]. This approach aims to secure national data assets while leveraging commercial innovation.

Development Drivers While specific locations of new hyperscale facilities are not detailed in current open-source intelligence, the expansion of data center capacity is driven by the *6G Bridge* program (2023–2026) and high digitalization rates in the SME sector [Source 1][Source 3]. The national strategy aligns with the EU’s Digital Decade goals, necessitating robust infrastructure to support advanced 5G and future 6G technologies.

2.4 Resilience and Physical Security

Submarine Cable Threats Finland’s international connectivity is heavily dependent on submarine cables in the Baltic Sea. This infrastructure faces elevated threats from geopolitical tensions. Recent incidents of cable damage in the region, linked to vessels associated with Russia and China, highlight the vulnerability of these assets to physical sabotage and “grey zone” activities [Source 1].

Regulatory Framework and Resilience To counter these threats, Finland is implementing EU-wide directives, specifically the Directive on the Resilience of Critical Entities (CER) and the NIS2 Directive. These frameworks mandate rigorous risk assessments and the implementation of technical and organizational security measures [Source 1]. However, challenges remain regarding the reliance on private operators for critical infrastructure and the need to secure supply chains against external exploitation [Source 2].

References

- [Source 1] Submarine Cable Security at Risk Amid Geopolitical Tensions (https://www.recordedfuture.con cables-face-increasing-threats)
- [Source 2] The Envy of Europe: Nordics Lead in 5G Availability and Network ... (https://www.ookla.com/articles/nordics-5g-q1-2025)
- [Source 3] Finnish Communication and Internet Exchange - Wikipedia (https://en.wikipedia.org/wiki/Fin
- [Source 4] Fibre optic connections available to nearly 2 million households (https://www.traficom.fi/en/nev optic-connections-available-nearly-2-million-households)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 3

Market

3.1 Market

Executive Summary

The Finnish telecommunications market is characterized by advanced infrastructure and exceptionally low consumer pricing, yet it faces significant headwinds related to market saturation and broader economic instability. Finland maintains a highly competitive pricing environment, with the average price of 1GB of mobile data standing at approximately $1.16, significantly lower than the global average of $8.53 and the UK average of $6.66 [Source 2 (Q2)]. While network performance is robust—marked by high "Consistent Quality" scores for major operators like Telia and Elisa [Source 1 (Q4)]—the sector is grappling with the commoditization of core services. Operators are facing stagnating Average Revenue Per User (ARPU) and inflationary pressures that erode profitability [Source 1 (Q8)]. Furthermore, the investment climate is tempered by a recent recession, a shrinking workforce, and regulatory complexities that may hinder foreign direct investment despite the country's innovation potential [Source 4 (Q11)].

3.2 Competitive Landscape and Pricing

The Finnish mobile market is mature and driven by intense price competition rather than service differentiation. The cost of connectivity is among the lowest in the developed world; at $1.16 per gigabyte, Finnish mobile data rates are a fraction of those in comparable markets [Source 2 (Q2)]. This low-pricing environment benefits consumers but places financial strain on operators.

While specific market share data for 2024 is opaque, the primary incumbents identified in network performance assessments are Telia Finland and Elisa Finland [Source 1 (Q4)]. There is no evidence of a new, significant "disruptor" entering the market to drive prices down further; rather, the low prices appear to be a structural feature of the existing competition [Source 1 (Q6)]. The market dynamics mirror global trends where core connectivity has become commoditized, making it difficult for operators to raise prices or differentiate their offerings, leading to flat or declining ARPU across the sector [Source 1 (Q8)].

3.3 Network Infrastructure and Performance

Finland's telecommunications infrastructure prioritizes reliability over raw peak speeds. Recent network experience reports highlight that Finnish operators, specifically Telia and Elisa, excel in "Consistent Quality" metrics. This indicates that the networks reliably support standard user requirements such as SD video, voice calls, and web browsing, as well as more demanding applications like HD video and group calling [Source 1 (Q4)].

In terms of speed, Finland ranks approximately 19th globally, with average speeds estimated around 92.27 Mbps [Source 2 (Q12)]. While not the fastest globally, the emphasis on consistency suggests a strategic focus on uniform user experience rather than peak throughput. This reliability is critical as users increasingly prioritize consistent connectivity for real-time applications over theoretical maximum speeds [Source 1 (Q4)].

3.4 Strategic Outlook and Investment Climate

The economic outlook for the Finnish telecom market is mixed. The sector is operating within a wider economic recession (2023-2024) driven by high inflation, rising interest rates, and weak export demand, which has dampened investment and consumer confidence [Source 4 (Q11)]. Additionally, the market faces long-term demographic challenges, including an aging population and a talent shortage that negatively impacts large foreign-owned companies [Source 4 (Q11)].

From a transactional perspective, the market is ripe for consolidation. Following broader European trends, M&A activity is expected to increase as operators seek to scale in response to fragmented markets and the need for capital efficiency. The focus is likely to be on in-market consolidation to realize fixed-cost synergies [Source 1 (Q10)]. However, foreign investors must navigate a regulatory environment that, while generally pro-competitive, involves complex permitting processes and FDI screening mechanisms that can delay market entry [Source 2 (Q11)].

References

- [Source 2 (Q2)] India beats UK and US on mobile data price - BBC (https://www.bbc.com/news/technolog 47416250)
- [Source 1 (Q4)] Global Mobile Network Experience Awards 2023 Opensignal (https://cdn.opensignal.com/public/data/reports/pdf-only/data-2023-02/2023_globalmobilenetworkexpe
- [Source 1 (Q6)] SiTime | The Precision Timing Company (https://www.sitime.com/)
- [Source 1 (Q8)] Perspectives from the Global Telecom Outlook 2024–2028 - PwC (https://www.pwc.com/gx/en/industries/tmt/telecom-outlook-perspectives.html)
- [Source 1 (Q10)] Preparing For A New Era In Telco M&A - Oliver Wyman (https://www.oliverwyman.com/our-expertise/insights/2025/nov/european-telco-ma-transformation-next-growth-wave.html)

- [Source 2 (Q11)] The Impact of Regulation on International Investment in Finland (https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/05/the-impact-of-regulation-on-international-investment-in-finland_852df409/b1bf8bee-en.pdf)
- [Source 4 (Q11)] 2025 Investment Climate Statements: Finland - State Department (https://www.state.gov/reports/2025-investment-climate-statements/finland)
- [Source 2 (Q12)] Honestly didn't expect Finland's internet global speedtest index is ... (https://www.reddit.com/r/Finland/comments/17ihd0a/honestly_didnt_expect_finlands_internet_glo
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 4

Localization

Executive Summary

Finland maintains a sophisticated digital infrastructure, ranking among the top nations globally in the UN E-Government Development Index alongside Denmark and South Korea due to its high-quality online services and human capacity [Source 4]. However, the nation faces significant strategic challenges regarding data localization and digital sovereignty. While Finland does not currently enforce strict legal mandates for data localization comparable to authoritarian regimes [Source 7], it is actively pursuing a "hybrid" sovereign cloud strategy. This approach aims to secure 100% of critical public sector data domestically by leveraging government-owned "core" data centers while utilizing private sector partnerships for non-classified workloads [Source 2].

The dominance of US hyperscalers, which control approximately 72% of the European cloud market, presents a critical vulnerability regarding extraterritorial legal risks [Source 3]. The application of the US CLOUD Act creates potential conflicts with EU GDPR requirements, exposing Finnish entities to compelled data disclosure and surveillance risks without adequate legal recourse [Source 11][Source 12]. Consequently, Finland's localization strategy is defined by a tension between reliance on global hyperscalers for scalability and the imperative to develop a national digital ecosystem and sovereign infrastructure to mitigate legal and security risks [Source 2][Source 9].

4.1 Sovereign Cloud Strategy and Infrastructure

The Finnish government has adopted a hybrid model to address the reliance on foreign cloud providers. This strategy distinguishes between critical and non-critical workloads to balance security with operational efficiency.

The Hybrid Model The core of Finland's localization strategy involves the government owning and operating "core" data centers dedicated to critical workloads. The explicit objective is to ensure that 100% of critical public sector data is stored within domestic borders [Source 2]. For non-classified workloads, the government utilizes a partnership model with the private sector.

This approach aligns with the European Union's Digital Decade Program, targeting 2030 goals for digital transformation and sovereignty [Source 2].

Infrastructure Development To support this strategy, significant investments are being made in local high-performance computing. A notable development is the ASP DC campus in Pori, Finland. This facility is designed to cater to high-performance computing and AI infrastructure, serving enterprises and cloud providers [Source 1]. While this expands domestic capacity, the market remains heavily skewed toward foreign providers; US hyperscalers (AWS, Azure, Google Cloud) dominate the broader European market, leaving European alternatives with a minority share [Source 3].

Challenges to Implementation The execution of this sovereign strategy faces hurdles, including high implementation costs, the complexity of integrating legacy systems, and the persistent risk of vendor lock-in with established global providers [Source 2].

4.2 Legal Framework and Extraterritorial Risks

Finland's localization posture is heavily influenced by the legal implications of cross-border data flows, particularly regarding the United States.

The US CLOUD Act vs. GDPR A primary strategic concern is the extraterritorial application of the US CLOUD Act, which allows US authorities to compel data access from US-based cloud providers regardless of where the data is physically stored [Source 12]. This creates a direct conflict with the EU General Data Protection Regulation (GDPR), which mandates adequate protection for personal data. Legal analysis suggests that for Finnish public sector entities, uploading confidential information to US-owned clouds could constitute unlawful disclosure, as US law enforcement access lacks adequate judicial review under Finnish standards [Source 11].

Sovereignty and Surveillance The risk extends beyond regulatory non-compliance to a loss of digital sovereignty. Finnish entities have limited legal recourse against US surveillance requests, and the potential for compelled disclosure of sensitive business documents or citizen data remains a critical vulnerability [Source 12]. Unlike some jurisdictions that have enacted specific data localization laws to counter this, Finland relies on the broader EU regulatory framework and its hybrid infrastructure strategy to mitigate these risks [Source 7].

4.3 National Digital Ecosystem

Finland is fostering a domestic digital ecosystem to support its localization goals, focusing on standardization and advanced technology adoption.

Strategic Initiatives The government is implementing the "Artificial Intelligence 4.0 Programme," which promotes the adoption of AI and digital technologies, specifically targeting Small and Medium-sized Enterprises (SMEs). This is complemented by a national standardization strategy intended to strengthen the competitiveness of Finnish companies and define national priorities in alignment with EU standards [Source 9][Source 10].

Network and Domain Administration Finland's internet traffic exchange relies on local infrastructure, including the presence of the DATAIX Internet Exchange Point in Helsinki [Source 6]. Regarding the national namespace, the .fi country-code top-level domain (ccTLD) is the standard for Finnish entities and is utilized within the higher education sector [Source 13]. However, the adoption of advanced security protocols within this domain remains low; for instance, the implementation of DANE and MTA-STS for SMTP encryption is described as "close to non-existent," indicating a potential gap in the secure localization of email infrastructure [Source 8].

References

- [Source 1] ASP DC: Pori Campus Data Center - Baxtel (https://baxtel.com/data-center/asp-dc-pori-campus)
- [Source 2] Sovereign data center strategy - Nokia (https://www.nokia.com/asset/i/215164/)
- [Source 3] Leave the Room: A Reality Check on European Cloud Alternatives (https://www.linkedin.com/pulse/leave-room-reality-check-european-cloud-alternatives-benjamin-hermann-nm4pe)
- [Source 4] Online connectivity improves, but digital inclusivity remains a challenge - UN DESA (https://www.un.org/en/desa/online-connectivity-improves-digital-inclusivity-remains-challenge)
- [Source 5] Internet Traffic Exchange (EN) - OECD (https://www.oecd.org/content/dam/oecd/en/publicat traffic-exchange_g17a21c7/5k918gpt130q-en.pdf)
- [Source 6] List of Internet exchange points by size - Wikipedia (https://en.wikipedia.org/wiki/List_of_Int
- [Source 7] Sovereignty and Data Localization - Belfer Center (https://www.belfercenter.org/publication/so and-data-localization)
- [Source 8] Enforcing SMTP encryption - Theseus (https://www.theseus.fi/bitstream/10024/752515/2/The
- [Source 9] Finland AI Strategy Report - AI Watch - European Commission (https://ai-watch.ec.europa.eu/countries/finland/finland-ai-strategy-report_en)
- [Source 10] POLICY BRIEF - Business Finland (https://www.businessfinland.fi/4907e4/globalassets/julka brief-1_2025_standardization-ecosystems.pdf)
- [Source 11] Mitigating the risk of US surveillance for public sector services in the cloud (https://policyreview.info/articles/analysis/mitigating-risk-us-surveillance-public-sector-services-cloud)
- [Source 12] What is the US CLOUD Act? The underestimated risk to European company data and digital sovereignty (https://www.sproof.com/en/what-is-the-us-cloud-act-the-underestimated-risk-to-european-company-data-and-digital-sovereignty/)
- [Source 13] Domain names, what do they say about your HigherEd Institution? (https://listedtech.com/blog/domain-names-what-do-they-say-about-your-highered-institution/)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 5

Security

Executive Summary

Finland maintains a robust strategic posture in the cyber domain, evidenced by its high standing in global preparedness indices. The nation is currently ranked 4th on the National Cyber Security Index (NCSI), reflecting a mature digital development level and strong central government implementation of cybersecurity policies [Source 1]. Despite this high-level strategic success, technical indicators reveal specific vulnerabilities within the national internet infrastructure. Notably, Finland exhibits a significantly low Domain Name System Security Extensions (DNSSEC) validation rate of approximately 7%, lagging considerably behind regional neighbors such as Sweden and Norway [Source 2]. Furthermore, analysis of the routing infrastructure identifies several critical Autonomous System Numbers (ASNs) acting as potential chokepoints with high dependency scores, suggesting a concentration of risk in specific telecommunications entities [Internal Graph]. While the legal and capacity-building frameworks are strong, the technical adoption of routing security standards like RPKI remains opaque due to a lack of definitive public data [Source 3].

5.1 Strategic Cyber Posture and Policy Framework

Finland's cybersecurity governance is characterized by a high degree of preparedness. The country holds the 4th position on the National Cyber Security Index (NCSI) with a score of 95.83. This performance is largely driven by a Digital Development Level of 85.76, indicating a positive correlation between Finland's general digital advancement and its security implementation [Source 1]. The NCSI methodology highlights Finland's effectiveness in preventing cyber threats and managing incidents at a central government level [Source 4].

While specific rankings for the ITU Global Cybersecurity Index (GCI) are not detailed in current reporting, Finland's performance in such indices is typically underpinned by comprehensive National Cybersecurity Strategies (NCSs) and robust legal frameworks addressing cybercrime and data protection [Source 5]. The operational focus of Finland's National Cyber Security

Centre (NCSC-FI) includes specialized sectors, such as healthcare cybersecurity, demonstrating a targeted approach to critical infrastructure defense [Source 6].

5.2 Routing Security and Infrastructure Dependencies

Analysis of Finland's Border Gateway Protocol (BGP) routing ecosystem reveals critical dependencies that could serve as single points of failure or targets for interdiction.

Critical Chokepoints Intelligence derived from dependency analysis identifies several Finnish ASNs with a `d.hege` score of 1.0, indicating 100% dependency in their BGP route propagation. These entities act as potential chokepoints for routing security: * KTAB-AS Karjaan Puhelin Oy (ASN 42343) * PYHANET-AS Pyhanet Oy (ASN 57359) * H2NEXUS-AS H2NEXUS LTD (ASN 215730) * MPYNET-AS MPY Telecom Oy (ASN 34263) * neve (ASN 58340)

Additionally, major entities such as DNA (ASN 16086) and ELISA-AS (ASN 719) serve as critical hubs, with DNA supporting 1,110 dependent ASNs and ELISA supporting 760 [Internal Graph].

Routing Security Standards There is a notable intelligence gap regarding the adoption of Resource Public Key Infrastructure (RPKI) and Mutually Agreed Norms for Routing Security (MANRS) within Finland. Current data does not provide a definitive validation rate for RPKI or a list of MANRS participants among Finnish Internet Service Providers (ISPs) [Source 3]. Consequently, the percentage of Finnish IP prefixes with RPKI Route Origin Authorizations (ROAs) configured is currently unreported [Internal Graph].

5.3 Domain Name System (DNS) Security

Finland's adoption of DNS security protocols is currently suboptimal compared to global and regional standards. The DNSSEC validation rate for Finnish domain names is approximately 7% of internet traffic. This figure is significantly lower than the rates observed in neighboring Nordic states, specifically Sweden and Norway, where validation rates exceed 80% [Source 2].

Historically, global averages for DNSSEC validation were estimated at 26% as early as 2016, suggesting that Finland's current rate of 7% represents a persistent lag in securing DNS query traffic against manipulation [Source 7]. Intelligence regarding specific DNS manipulation attempts or anomalies originating from Finnish ASNs remains unavailable at this time [Internal Graph].

5.4 Threat Landscape and Incident Response

Specific metrics regarding the volume of malware-infected devices, botnet activity originating from Finland, or the scale of Distributed Denial of Service (DDoS) attacks targeting the nation are not definitively available in open-source reporting [Source 8]. While global threat intelligence reports from major vendors (e.g., Nokia, Check Point) track these trends broadly, they do not currently offer a granular breakout for Finland [Source 9].

Regarding incident response, there are no publicly available after-action reports detailing the NCSC-FI's effectiveness in mitigating large-scale BGP hijacking or widespread DDoS attacks. However, the NCSC-FI remains active in international forums, sharing best practices on sector-specific defense, particularly in securing healthcare infrastructure [Source 6].

References

- [Source 1] NCSI :: Ranking - National Cyber Security Index (https://ncsi.ega.ee/ncsi-index/)
- [Source 2] Traficom promotes the deployment of DNSSEC (https://www.traficom.fi/en/news/traficom-promotes-deployment-dnssec)
- [Source 3] routing security - bgp incidents, mitigation techniques and ... - OECD (https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/10/routing-security_15b121f7/40be69c8-en.pdf)
- [Source 4] National Cyber Security Index - EU Cyber Direct (https://eucyberdirect.eu/good-cyber-story/national-cyber-security-index)
- [Source 5] Global Cybersecurity Index 2024 - ITU (https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf)
- [Source 6] Conference Program / 31st Annual FIRST Conference (https://www.first.org/conference/2019/
- [Source 7] A quick review of DNSSEC Validation in today's Internet - Geoff Huston (https://www.potaroo.net/presentations/2016-06-27-dnssec.pdf)
- [Source 8] Annual Threat Assessment of the U.S. Intelligence Community (https://www.dni.gov/files/ODN
2025-Unclassified-Report.pdf)
- [Source 9] Nokia Threat Intelligence Report finds malicious IoT botnet activity ... (https://www.nokia.com/newsroom/nokia-threat-intelligence-report-finds-malicious-iot-botnet-activity-has-sharply-increased/)
- [Internal Graph] Internal Knowledge Graph (Dependency and Routing Data)

Chapter 6

Governance

Executive Summary

Finland maintains a sophisticated governance framework for the digital domain, characterized by a strong legal commitment to connectivity and strict adherence to European Union regulatory standards. Unlike many global counterparts, Finland has established internet access as a legal right for its citizens, a policy stance that precludes the use of internet shutdowns or widespread blocking of social media platforms [Source 2]. The nation's data protection regime is fully aligned with the General Data Protection Regulation (GDPR), ensuring rigorous oversight of personal data processing by state and commercial entities [Source 1].

However, the governance landscape is marked by an ongoing tension between privacy rights and national security imperatives. While Finland ratified the Council of Europe Convention on Cybercrime (Budapest Convention) in 2007 [Source 1], recent legislative shifts—specifically the intelligence laws effective since 2019—have expanded state capacity for bulk interception of cross-border communications [Source 1]. Furthermore, the implementation of the Cybersecurity Act in April 2025, aligning with the EU's NIS2 Directive, signals a tightening of security requirements for essential entities [Source 1]. Current parliamentary debates continue to scrutinize the balance between the "Digital Welfare State" model and the expansion of surveillance powers [Source 1].

6.1 Legal Framework for Digital Rights and Access

Finland's governance of the digital sphere is anchored in the principle of universal access. The state has formally recognized internet access as a legal right, a distinction shared regionally with Estonia [Source 2]. Consequently, there is no evidence of internet shutdowns or the widespread blocking of social media platforms within the last five years [Source 2].

Freedom of expression is protected by law, yet the legal system faces challenges in addressing online harms. The governance framework is currently tested by the need to balance free speech with protections against online harassment and hate speech. This is particularly acute regarding coordinated harassment campaigns targeting government ministers and the activities of extremist groups like the Nordic Resistance Movement, which have faced charges for incitement and illegal association [Source 1].

Data privacy is governed by the EU General Data Protection Regulation (GDPR) (EU) 2016/679, which mandates strict integrity and confidentiality in data processing. The Finnish Data Protection Ombudsman serves as the primary supervisory authority for these regulations [Source 1]. Non-compliance with these standards carries significant penalties, ranging from €10 million to €20 million, or up to 4% of a company's total worldwide annual turnover [Source 3].

6.2 Cybersecurity and Surveillance Architecture

Finland's cybersecurity governance is integrated into international and European frameworks. The country ratified the Budapest Convention on May 24, 2007, which entered into effect on September 1, 2007, facilitating international cooperation on cybercrime [Source 1].

Domestically, the **Finnish Criminal Code (39/1889)** and the **Act on Electronic Communications Services (917/2014)** provide the statutory basis for prosecuting data offenses and regulating communications security [Source 1]. A significant evolution in this framework occurred with the enactment of intelligence laws in 2019, which introduced provisions for the bulk interception of cross-border electronic communications. This expansion of state power has been a subject of parliamentary debate, reflecting concerns over the "shrinking space for privacy" and the historical legacy of "Lex Nokia," legislation that previously expanded corporate surveillance rights [Source 1, Source 2].

Most recently, the **Cybersecurity Act**, which entered into force in April 2025, implements the EU's NIS2 Directive. This legislation mandates high cybersecurity standards for providers of essential services, further integrating Finland's national security posture with broader EU resilience strategies [Source 1].

6.3 Regulatory Oversight and Licensing

The governance of telecommunications infrastructure is centralized under the Finnish Transport and Communications Agency (Traficom). The licensing process for operations such as earth stations and radar requires applicants to demonstrate technical prerequisites through a formal application process [Source 2].

While the licensing process is generally administrative, it contains a specific mechanism for political intervention. If the issuance of a telecommunications license is deemed to have implications for national security, the decision-making authority shifts from the agency directly to the Government [Source 2]. This provision ensures that the executive branch retains control over critical infrastructure components that may impact the state's strategic interests.

References

- [Source 1] UNTC (https://treaties.un.org/Pages/showDetails.aspx?objid=0800000280071e5b&clang=_en
- [Source 1] Internet shutdowns in international law | Global Freedom of Expression (https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2023/06/Internet-shutdowns-in-international-law.pdf)
- [Source 2] The Changing Landscape of Internet Shutdowns in Africa (https://ora.ox.ac.uk/objects/uuid:6a
7b23-44e1-b6c2-e73a335024e1/files/s0p096822r)
- [Source 1] Cybersecurity Laws and Regulations Report 2026 Finland - ICLG.com (https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/finland)
- [Source 2] Licences for earth station and radar operations - Traficom (https://www.traficom.fi/en/commun
licences-and-frequencies/frequency-planning-and-use/licences-earth-station-and)
- [Source 1] GDPR Countries in 2026 | GDPR Advisor - GDPR Consultant (https://www.gdpradvisor.co.uk/
countries)
- [Source 3] Data Protection in Transition: GDPR, CCPA and Comparable ... - DFIN (https://www.dfinsolutions.com/knowledge-hub/thought-leadership/article/data-protection-transition-gdpr-ccpa-and-comparable-data)
- [Source 1] Operationalising communication rights: the case of a “Digital Welfare ... (https://policyreview.info/articles/analysis/operationalising-communication-rights-case-digital-welfare-state)
- [Source 1] a comparative analysis of the debates in UK, Finland and Norway (https://link.springer.com/article/10.1057/s41284-024-00443-3)
- [Source 1] 2022 Country Reports on Human Rights Practices: Finland (https://www.state.gov/reports/20
country-reports-on-human-rights-practices/finland)
- [Source 2] Online Harassment Is Not Gender-Neutral - the United Nations (https://www.un.org/en/un-chronicle/online-harassment-not-gender-neutral)

Chapter 7

Strategic Synthesis & Roadmap

Chapter 8

Section 7: Strategic Synthesis & Roadmap

To: The President of the Republic / The Prime Minister **From:** Chief Strategy Officer **Date:** October 26, 2025 **Subject:** STATE OF THE NETWORK – From “Digital Island” to “Digital Fortress”

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

The Narrative: Surface Excellence, Subsurface Fragility Finland stands at a critical strategic juncture. On the surface, we are a global exemplar of digital advancement: we possess near-ubiquitous 5G coverage, the world’s most affordable mobile data ($1.16/GB), and a governance model that enshrines internet access as a human right. We are a “Digital Superpower.”

However, beneath this veneer lies a dangerous paradox. **We are a digital island relying on a glass bridge.** Our geopolitical reality—a frontline state bordering a hostile Russia—clashes with our infrastructure reality. We rely heavily on a limited number of subsea cables (C-Lion1, Balticconnector) that have already been targeted by sabotage. Simultaneously, our logical infrastructure is dangerously centralized; a single US entity (Cloudflare) and a handful of domestic operators hold the keys to our global connectivity.

The Paradox: > **“Strong Infrastructure but Weak Hygiene.”** > While we have built massive 5G highways, we have failed to secure the on-ramps. Our DNSSEC validation rate (7%) is an anomaly compared to our Nordic neighbors (>80%), and our routing security is opaque. We have built a high-speed digital economy, but left the back doors unlocked and the physical cables exposed.

8.2 2. SWOT Analysis: The Strategic Cheat Sheet

8.2.1 Strengths (Internal Assets)

- **Mobile Ubiquity:** 96% household coverage for high-speed 4G/5G; we have successfully deployed the "invisible highways."
- **Cost Competitiveness:** Lowest data prices in the developed world drive massive consumer adoption and digitalization.
- **Trusted Governance:** High trust in public institutions allows for the implementation of the "Hybrid Sovereign Model" (Gov core + Private edge) without public backlash.
- **Energy & Climate:** Stable green energy grid makes Finland an ideal host for high-performance computing (e.g., Pori Campus).

8.2.2 Weaknesses (Internal Flaws)

- **Technical Hygiene Gap:** Abysmal DNSSEC adoption (7%) and low RPKI validation leave the nation vulnerable to spoofing and route hijacking.
- **Centralization Risk:** The market is an oligopoly (Elisa, DNA, Telia). While efficient, this creates massive "Single Points of Failure."
- **Rural Divide:** The sharp contrast between urban fiber and rural "white spots" creates a two-tier society, weakening national cohesion in border regions.
- **Dependency Chokepoints:** Over-reliance on Cloudflare (956 dependencies) and GlobalConnect creates logical bottlenecks we do not control.

8.2.3 Opportunities (External Trends)

- **The "Digital North" Alliance:** Leveraging Nordic cooperation to create a shared, redundant mesh network that Russia cannot easily sever.
- **NATO Integration:** Utilizing our position to become the "Data Bunker" for NATO's Arctic flank, securing funding for dual-use infrastructure.
- **Sovereign AI:** The *6G Bridge* program and AI 4.0 initiatives position Finland to lead in specialized, sovereign AI, reducing reliance on US tech.

8.2.4 Threats (External Dangers)

- **Seabed Warfare:** Active sabotage of Baltic cables (C-Lion1) by "grey zone" actors (Russia/China) threatens to sever us from Europe.
- **Legal Extraterritoriality:** The US CLOUD Act conflicts with GDPR, meaning Finnish public data in US clouds (AWS/Azure) is legally vulnerable to foreign surveillance.
- **Economic Stagnation:** Global recession and local market saturation (low ARPU) limit the private sector's ability to fund necessary security upgrades without state intervention.

8.3 3. Strategic Roadmap: The Policy Agenda

8.3.1 Phase 1: Immediate - "The Hygiene Mandate" (0 - 12 Months)

- **Objective:** Close the technical security gap with Sweden and Norway at zero cost to the taxpayer.
- **Action 1 (Executive Decree):** Mandate **DNSSEC and RPKI adoption** for all Critical Infrastructure Providers and ISPs. We cannot allow our validation rate to remain at 7%.
- **Action 2 (Audit):** Order a classified "Dependency Audit" on **Cloudflare and Global-Connect**. We must know exactly which government services go dark if these two entities fail.
- **Action 3 (Resilience):** Enforce **NIS2 Directive** compliance immediately. Shift the burden of security from the user to the operator (Elisa, DNA, Telia).

8.3.2 Phase 2: Medium Term - "Physical & Logical Redundancy" (1 - 3 Years)

- **Objective:** Eliminate the "Island" risk.
- **Action 1 (Infrastructure):** Commission the **"Arctic Link"**. Accelerate fiber routes north through Norway/Sweden to the Atlantic, bypassing the vulnerable Baltic Sea entirely.
- **Action 2 (Sovereignty):** Operationalize the **"Hybrid Sovereign Cloud."** Ensure 100% of classified and critical public sector data is migrated to government-owned data centers, insulating it from the US CLOUD Act.
- **Action 3 (Market):** Incentivize **Rural Fiber Rollout** in Eastern border regions. A connected border population is a secure border population; we cannot have "dead zones" near Russia.

8.3.3 Phase 3: Long Term - "The Data Bunker of the North" (3 - 5 Years)

- **Objective:** Turn security into an export product.
- **Action 1 (Vision):** Position Finland as the **Global Safe Haven for Data**. Leverage our bedrock stability, green energy, and NATO status to attract hyperscalers to build *sovereign* regions here, not just standard availability zones.
- **Action 2 (Innovation):** Lead the **6G Standardization**. Ensure the next generation of protocols has security baked in (unlike the current BGP/DNS flaws), preventing future vulnerabilities.

8.4 4. Final Verdict

8.4.1 Investability Score: MEDIUM-HIGH

- **Explanation:** Finland offers a stable, high-tech environment with incredibly low barriers to entry for digital services. However, the market is saturated (commoditized connectivity), and ARPU is low. The real investment opportunity lies not in selling connectivity, but in **Data Center Infrastructure** and **Cybersecurity Solutions** catering to the sovereign needs of Europe.

8.4.2 Maturity Score: MATURE (But Complacent)

- **Explanation:** We are a mature digital society with an "Emerging" security mindset. We have rested on the laurels of our high 5G rankings while neglecting the plumbing (routing security). We are a Ferrari with the doors unlocked. The technology is world-class; the security posture must now rise to match it.