STRATEGIC COUNTRY REPORT: SWEDEN

Automated Strategic Analyst (v2.2 Parallel)

12 February 2026

Contents

1 Geopolitics **3**
Executive Summary . . . 3
1.1 Strategic Posture and Digital Sovereignty . . . 3
1.2 Critical Infrastructure and Hybrid Threats . . . 4
1.3 Network Topology and Dependency Analysis . . . 4
1.4 Regulatory Framework and Foreign Investment . . . 5
References . . . 5

2 Infrastructure **7**
Executive Summary . . . 7
Mobile Network Infrastructure . . . 7
Fixed Broadband and National Strategy . . . 8
Data Center and Internet Architecture . . . 8
References . . . 9

3 Market **10**
Executive Summary . . . 10
3.1 Market Structure and Competitive Landscape . . . 10
3.2 Network Infrastructure and Performance . . . 11
3.3 Economic Outlook and Strategic Trends . . . 11
References . . . 12

4 Localization **13**
Executive Summary . . . 13
4.1 Cloud Infrastructure and Market Dynamics . . . 13
4.2 Legal Framework and Jurisdictional Risks . . . 14
4.3 Public Sector and E-Government Sovereignty . . . 14
4.4 Domain Name Ecosystem (.se) . . . 15
References . . . 15

5 Security **17**
Executive Summary . . . 17
5.1 Network Topology and Infrastructure Vulnerabilities . . . 17
5.2 Routing Security and RPKI Implementation . . . 18
5.3 Threat Landscape and Incident History . . . 18
References . . . 18

6 Governance **20**
Executive Summary . . . 20
6.1 Legal Framework for Digital Rights and Data Privacy . . . 20
6.2 Cybercrime and International Cooperation . . . 21

6.3 Electronic Commerce and Telecommunications Regulation 21
6.4 Strategic Governance Outlook 21
References 22

7 Strategic Synthesis & Roadmap 24

8 Section 7: Strategic Synthesis & Roadmap 25
8.1 1. Executive Summary: The “Big Picture” Diagnosis 25
8.2 2. SWOT Analysis: The Strategic Cheat Sheet 25
8.3 3. Strategic Roadmap: The Policy Agenda 26
8.4 4. Final Verdict 27

Chapter 1

Geopolitics

Executive Summary

Sweden's geopolitical position in the digital domain is defined by its integration into the European Union's regulatory framework and its frontline status in the Baltic Sea security complex. The nation's digital sovereignty strategy is characterized by a dual approach: fostering an open, innovative digital market while aggressively countering authoritarian state ambitions and hybrid threats [Source 2 - Govt.se]. Recent kinetic incidents involving submarine cables in the Baltic Sea have elevated the protection of physical digital infrastructure to a primary national security objective, highlighting vulnerabilities to sabotage by foreign adversaries [Source 2 - CNBC].

While Sweden possesses a robust and diverse network topology with 889 distinct upstream providers, it retains significant dependencies on major international transit providers such as Cogent Communications and Telia Carrier [Internal Graph]. Furthermore, intelligence indicates a reliance on Autonomous Systems (ASNs) associated with high geopolitical risk scores, suggesting potential exposure to instability originating from rival nations [Internal Graph]. Sweden's policy framework is heavily influenced by EU directives, specifically regarding critical entity resilience and data protection, positioning the country as a staunch advocate for a rules-based global digital order [Source 1 - Europarl].

1.1 Strategic Posture and Digital Sovereignty

Sweden's geopolitical stance on digital issues is aligned with the European Union's "Open Strategic Autonomy." The government actively advocates for a digital future that supports free data flow and market competition, explicitly positioning itself against the "digital sovereignty" models promoted by authoritarian regimes which emphasize state control [Source 2 - Govt.se]. Key objectives include strengthening national resilience against hybrid operations, combating digital trade barriers, and fostering an environment conducive to innovation and entrepreneurship [Source 1 - WEF].

Regionally, Sweden is a central actor in Nordic digital cooperation. Through the Nordic Council of Ministers, Sweden participates in initiatives to leverage digitalization for sustainable regional development, ensuring its national strategies complement broader Nordic and EU Digital Decade targets [Source 1 - Nordregio]. Internationally, Sweden is engaged in standardization processes to counter the growing influence of authoritarian states in setting global technical norms [Source 2 - Govt.se].

1.2 Critical Infrastructure and Hybrid Threats

The security of Sweden's physical digital infrastructure has become a focal point of geopolitical tension. The Baltic Sea is increasingly viewed as a theater for hybrid warfare, evidenced by the severing of the BCS East-West Interlink (connecting Lithuania and Sweden) and a telecom cable connecting Sweden and Estonia in late 2023 and 2024 [Source 2 - CNBC]. Investigations into these incidents have focused on the potential involvement of Russian and Chinese vessels, raising concerns about state-sponsored sabotage targeting Western critical infrastructure [Source 3 - CSIS].

While the specific ownership structures of Sweden's landing stations are not publicly detailed in the available intelligence, the sector is characterized by a mix of private commercial operators (e.g., suppliers like Alcatel Submarine Networks) subject to increasing governmental oversight [Source 1 - Recorded Future]. The concentration of cable systems along similar geographic routes in the Baltic Sea increases vulnerability to targeted attacks. However, the impact of recent cable cuts was mitigated by European network redundancy, preventing a complete loss of connectivity [Source 1 - Recorded Future].

1.3 Network Topology and Dependency Analysis

Sweden's internet infrastructure exhibits a high degree of resilience in terms of provider diversity. The core infrastructure is transited by 889 distinct upstream Autonomous System Numbers (ASNs), a figure that suggests a low vulnerability to single-point failures [Internal Graph]. However, the upstream connectivity market is concentrated; AS6939 (likely Cogent Communications) and AS2914 (likely Telia Carrier) are the most significant providers, with 62,351 and 25,559 dependent ASNs respectively [Internal Graph].

Despite this robustness, network analysis reveals potential geopolitical vulnerabilities. Swedish ASNs show significant dependencies on foreign ASNs located in countries with high geopolitical risk scores (d.hege $>$ 0.8). Furthermore, major dependencies include global entities such as Cloudflare, CDN77, and SpaceX-Starlink, highlighting a reliance on infrastructure that transcends national borders and may be subject to extraterritorial jurisdiction or geopolitical instability [Internal Graph].

1.4 Regulatory Framework and Foreign Investment

Sweden’s approach to foreign investment in critical digital infrastructure is governed by its commitment to national security and EU obligations. As an EU member state, Sweden adheres to the Directive on the Resilience of Critical Entities (CER), which mandates the implementation of technical and organizational measures to enhance resilience against physical and cyber threats [Source 1 - EC].

The national strategy acknowledges that public and private actors are regular targets of foreign power cyberattacks intended to disrupt services or gather intelligence [Source 2 - Govt.se]. Consequently, while Sweden promotes an open investment climate, the policy framework implies rigorous scrutiny of foreign involvement in critical infrastructure to prevent compromise by adversarial states. This is reinforced by Sweden’s adherence to the EU’s General Data Protection Regulation (GDPR) and the Digital Services Act (DSA), which collectively structure the legal environment for cross-border data flows and digital platform operations [Source 1 - Europarl].

References

- [Source 1 - Recorded Future] Submarine Cable Security at Risk Amid Geopolitical Tensions &amp (https://www.recordedfuture.com/research/submarine-cables-face-increasing-threats)
- [Source 1 - Atlantic Council] How allied Sweden and Finland can secure Northern Europe (https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/how-allied-sweden-finland-can-secure-northern-europe/)
- [Source 1 - WEF] What is digital sovereignty and how are countries approaching it? (https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/)
- [Source 1 - Europarl] EU’s trade and digital economy – Challenges and opportunities for ... (https://www.europarl.europa.eu/RegData/etudes/STUD/2025/754479/EXPO_STU(2025)754479_EN.
- [Source 1 - EC] Critical infrastructure resilience at EU-level (https://home-affairs.ec.europa.eu/policies/int security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en)
- [Source 1 - Nordregio] Digitalisation as a tool for sustainable Nordic regional development (https://nordregio.org/app/uploads/2018/02/Digitalisation-as-a-tool-for-sustainable-Nordic-regional-development-Preliminary-literature-and-policy-review.pdf)
- [Source 2 - Govt.se] Sweden in a digital world - Government.se (https://www.government.se/contentassets/ in-a-digital-world—a-strategy-for-swedens-foreign-and-security-policy-on-cyber-and-digital-issues.pdf)
- [Source 2 - CNBC] Explainer: Baltic Sea undersea cable cuts stoke geopolitical tensions (https://www.cnbc.com/2024/11/28/explainer-baltic-sea-undersea-cable-cuts-stoke-geopolitical-tensions.html)
- [Source 3 - CSIS] Safeguarding Subsea Cables: Protecting Cyber Infrastructure ... - CSIS (https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-

infrastructure-amid-great-power-competition)

- [Source 3 - FCC] Federal Communications Commission FCC 24-119 Before the ... (https://docs.fcc.gov/public/attachments/FCC-24-119A1.pdf)
- [Source 4 - NORDUnet] The History of nordunet (https://nordu.net/wp-content/uploads/2023/11/TheHi
- [Internal Graph] IYP-GRAPH - Internal Knowledge Graph Data

Chapter 2

Infrastructure

Executive Summary

Sweden maintains a highly advanced telecommunications and digital infrastructure posture, characterized by aggressive government targets and substantial private sector investment. The nation has achieved near-ubiquitous mobile connectivity, with major operators reporting 5G population coverage reaching 99.9%, effectively matching existing 4G footprints [Source 2]. In the fixed-line sector, Sweden ranks third in Europe for Fiber-to-the-Home (FTTH) penetration, driven by proactive state intervention and the "Completely Connected Sweden by 2025" strategy [Source 3, Source 4].

While the physical internet architecture remains heavily centralized around Stockholm-based Internet Exchange Points (IXPs) [Source 6], there is a strategic northward expansion of data center capacity. The Arctic region is increasingly utilized for high-performance computing (HPC) and AI-driven workloads, leveraging green energy and low temperatures [Source 7, Source 8]. Despite this progress, challenges remain regarding spectrum optimization for smaller operators and the maintenance of consistent network quality across sparsely populated regions [Source 5].

Mobile Network Infrastructure

5G Deployment and Coverage Sweden's mobile infrastructure has undergone a rapid upgrade cycle. Through the Net4Mobility joint venture, operators Tele2 and Telenor have reported a 5G population coverage of 99.9%, asserting that next-generation coverage now mirrors the extent of the legacy 4G network [Source 2]. This expansion has been facilitated by the activation of the 700 MHz low-frequency band, which is critical for penetrating building structures and covering vast, sparsely populated rural areas that characterize the Swedish terrain [Source 2]. This deployment strategy aligns with broader Nordic policies designed to extend widespread rollout beyond core urban centers [Source 1].

Spectrum and Network Quality While coverage metrics are high, technical analyses suggest underlying challenges in spectrum utilization. Reports indicate that smaller operators face spectrum limitations, and certain bands, such as 1800 MHz, have historically been underutilized [Source 5]. Strategic analysis advocates for a shift in performance metrics from simple peak speeds to "Consistent Quality" indicators (latency, jitter, packet loss) to better assess network resilience [Source 5].

Fixed Broadband and National Strategy

Fiber Penetration and Targets Sweden is a global leader in fiber deployment. As of September 2021, the FTTH/B penetration rate stood at 64.4%, placing the country third in the European region [Source 3]. This high adoption rate is attributed to early and proactive state intervention favoring fiber expansion over copper legacy systems [Source 3].

"Completely Connected Sweden by 2025" The government's primary infrastructure directive, "Completely Connected Sweden by 2025," is overseen by the Ministry of Climate and Enterprise and the Swedish Post and Telecom Authority (PTS) [Source 4]. The strategy mandates the following objectives for 2025: * 98% of households and businesses must have access to 1 Gbps broadband. * The remaining 2% must have access to at least 100 Mbps or 30 Mbps. * Reliable, high-quality mobile services must cover the entire country [Source 4].

To facilitate these goals, the *Bredbandsforum* was established to coordinate efforts between the government, commercial entities, and regional authorities to remove deployment barriers [Source 4].

Data Center and Internet Architecture

Regional Hubs and AI Expansion Sweden's data center industry is pivoting toward high-performance computing (HPC) to support the growing demand for Artificial Intelligence (AI) and cloud services. While there is no public map of all facilities, intelligence indicates a strategic concentration in the Arctic region, specifically Kiruna and Boden [Source 8].

A notable development is the expansion by HIVE Digital Technologies in Boden. The operator is converting a Tier-1 facility into a Tier-3 liquid-cooled HPC center aimed at enterprise-grade AI and GPU cloud workloads. This facility, along with operations in Stockholm, supports the projection of operating approximately 6,000 GPUs globally by 2026 [Source 7]. Additionally, NVIDIA is establishing AI technology centers in the region to bolster digital sovereignty and infrastructure [Source 9].

Internet Exchange Points (IXPs) The core routing infrastructure remains centralized. The primary active Internet Exchange Points identified are Netnod, STHIX, and FSN, all of which are located in Stockholm [Source 6]. This geographic concentration presents a potential single-point-of-failure risk, although the distributed nature of the northern data centers offers some redundancy for storage and compute capabilities.

References

- [Source 1] The Envy of Europe: Nordics Lead in 5G Availability and Network ... (https://www.ookla.com/articles/nordics-5g-q1-2025)
- [Source 2] Tele2 and Telenor now activate 5G across the entire mobile network (https://www.tele2.com/media/news/2025/tele2-and-telenor-now-activate-5g-across-the-entire-mobile-network-covering-90-of-swedens-landmass-and-99-9-of-the-population/)
- [Source 3] FTTH/B Global Ranking 2022 - FTTH Council Europe (https://www.ftthcouncil.eu/knowledge centre/all-publications-and-assets/1463/ftth-b-global-ranking)
- [Source 4] Digital connectivity in Sweden | Shaping Europe's digital future (https://digital-strategy.ec.europa.eu/en/policies/digital-connectivity-sweden)
- [Source 5] Scandinavia Report 2019 - Tutela (https://www.tutela.com/hubfs/Assets/Nordics%20State%20 %20January%202019.pdf)
- [Source 6] List of Internet exchange points - Wikipedia (https://en.wikipedia.org/wiki/List_of_Internet_
- [Source 7] HIVE Digital Technologies Ltd (https://www.hivedigitaltechnologies.com/news/hive-digital-technologies-surpasses-22-ehs-and-accelerates-conversion-from-tier-1-to-tier-3-data-centers-for-ai-cloud-expansion-in-sweden/)
- [Source 8] Sweden's Arctic Advantages: Critical Minerals, Space, and Data (https://www.wilsoncenter.org arctic-advantages-critical-minerals-space-and-data)
- [Source 9] Europe Builds AI Infrastructure With NVIDIA to Fuel Region's Next ... (http://nvidianews.nvidia.com/news/europe-ai-infrastructure)

Chapter 3

Market

Executive Summary

The Swedish telecommunications market represents a mature, highly concentrated oligopoly characterized by advanced digital infrastructure and stable competitive dynamics. The sector is dominated by four incumbent operators—Telia, Tele2, Telenor, and Three—who collectively control approximately 96% of the mobile subscriber market and 89% of the fixed broadband market [Source 1]. Unlike markets characterized by aggressive price wars, Sweden exhibits a trend of price alignment and brand value retention, with no significant "disruptor" currently challenging the established order [Source 2].

Infrastructure performance remains a strategic asset for the nation. Recent assessments indicate robust network capabilities, with median mobile download speeds reaching 133.93 Mbps and fixed broadband speeds averaging 149.71 Mbps [Source 3]. While the market offers a positive outlook for investors driven by high digital literacy and 5G expansion, it faces headwinds from intense competition, regulatory complexities regarding EU cloud certification, and pressure on equipment manufacturers like Ericsson [Source 4, Source 5].

3.1 Market Structure and Competitive Landscape

The Swedish market structure is defined by high barriers to entry and significant consolidation. The competitive landscape is stabilized by a "Big Four" dynamic comprising Telia, Tele2, Telenor, and Three. These operators maintain a stranglehold on the sector, evidenced by the Swedish Post and Telecom Authority (PTS) reporting that 96% of mobile subscriptions and 89% of fixed broadband subscriptions are held by these few large players [Source 1].

Competitive Intensity and Pricing Despite the presence of four major players, the market does not exhibit the characteristics of a fragmented sector. Intelligence indicates a lack of a significant "disruptor" entity actively driving down prices. Instead, the market trajectory suggests price alignment among major operators, who focus on maintaining brand value and premium positioning rather than engaging in race-to-the-bottom pricing strategies [Source 2].

Established brands like Telia continue to command high value, leveraging their market position to sustain revenue streams without aggressive discounting [Source 2].

Revenue and Profitability Metrics Assessing precise Average Revenue Per User (ARPU) remains challenging due to inconsistencies in reporting standards across the Nordic region. Specifically, the classification of Fixed Wireless Access (FWA)—reported as fixed broadband in some jurisdictions but mobile in Sweden—complicates direct revenue comparisons and obscures a definitive ARPU figure for Swedish operators [Source 6]. However, the dominance of the major players suggests that revenue market share closely mirrors subscriber share.

3.2 Network Infrastructure and Performance

Sweden continues to prioritize high-quality connectivity, positioning itself as a leader in digital infrastructure.

Speed and Latency Network performance metrics for the first half of 2025 and mid-2024 highlight strong throughput capabilities: * **Mobile (4G/5G):** Median download speeds are recorded at 133.93 Mbps, with upload speeds at 17.07 Mbps [Source 3]. * **Fixed Broadband:** Median download speeds stand at 149.71 Mbps, with upload speeds at 48.83 Mbps [Source 3].

Quality of Experience Beyond raw speed, the quality of service for real-time applications is a critical differentiator. Telenor has been identified as a leader in 5G gaming experience, a key proxy for network latency and consistency [Source 7]. This suggests that while all major operators provide high bandwidth, differentiation is increasingly occurring in the stability and latency domains required for next-generation applications.

3.3 Economic Outlook and Strategic Trends

Investment Climate From an investor perspective, the Swedish telecom market offers a mixed but generally positive outlook. The country's high rate of digital innovation and nearly universal broadband access provide a fertile ground for the growth of the Internet of Things (IoT) and advanced digital services [Source 4]. However, the market is not immune to broader economic pressures. Ericsson, a bellwether for the Swedish telecom sector, has reported year-on-year sales declines, highlighting the competitive pressures within the equipment and infrastructure segment [Source 5].

Regulatory and Structural Challenges Operators face an evolving regulatory landscape, particularly regarding integration with the European Union's digital frameworks. Challenges related to public procurement of cloud solutions and the EU Cloud Services Cyber Security Certification Scheme create complexity for both domestic and foreign investors [Source 4].

Future Market Trajectory While specific recent M&A activity within Sweden is not highlighted in current reporting, the market is influenced by global Technology, Media, and Telecommunications (TMT) trends. These include a pivot toward Artificial Intelligence (AI) infrastructure and a strategic focus on core assets. Operators are expected to prioritize capital efficiency, potentially leading to further infrastructure consolidation or portfolio separation to fund AI and fiber network expansion [Source 8].

References

- [Source 1] The Swedish Telecommunications Market 2023 (https://statistik.pts.se/media/2iznynpq/the-swedish-telecommunications-market-2023-dnr24-192-en_t.pdf?utm)
- [Source 2] Kantar BrandZ Top 30 Most Valuable Swedish Brands 2023 ranking (https://www.kantar.com/inspiration/brands/inaugural-kantar-brandz-top-30-most-valuable-swedish-brands-2023-ranking)
- [Source 3] Sweden's Mobile and Broadband Internet Speeds (https://www.speedtest.net/global-index/sweden)
- [Source 4] Sweden - Digital Economy - International Trade Administration (https://www.trade.gov/countr commercial-guides/sweden-digital-economy)
- [Source 5] European markets live updates: stocks, news, data and earnings (https://www.cnbc.com/2024/1 markets-live-updates-stocks-news-data-and-earnings.html)
- [Source 6] Assessment of Norwegian fixed broadband pricing in a Nordic context (https://www.regjeringen.no/contentassets/311eeb54f87341d187b04361c7f62038/assessment-of-norwegian-fixed-broadband-pricing-in-a-nordic-context-by-tefficient-5-sep-2024.pdf)
- [Source 7] Speedtest® Connectivity Report | Sweden H1 2025 - Ookla (https://www.ookla.com/research/re speedtest-connectivity-report-h1-2025)
- [Source 8] Global M&A trends in technology, media and telecommunications (https://www.pwc.com/gx/en/services/deals/trends/telecommunications-media-technology.html)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 4

Localization

Executive Summary

Sweden occupies a paradoxical position in the digital domain: it is a global leader in e-government and digital adoption yet faces acute vulnerabilities regarding data localization and infrastructure sovereignty. The nation's digital ecosystem is characterized by a heavy reliance on foreign hyperscalers—primarily United States-based providers like AWS, Microsoft Azure, and Google Cloud—which dominate the market at the expense of local European alternatives [Source 12]. This dependency creates significant legal and strategic risks, particularly concerning the extraterritorial reach of U.S. surveillance laws such as the CLOUD Act and FISA Section 702, which conflict directly with the European Union's General Data Protection Regulation (GDPR) [Source 13].

While Sweden does not have specific legislation mandating data localization for all sectors, strict regulatory interpretations by the Swedish Data Protection Authority (IMY) regarding international data transfers have created a de facto localization requirement for sensitive public sector data [Source 13] [Source 14]. The public sector currently faces a "deadlock," balancing the operational need for modern cloud services against the legal imperative to protect citizen data from foreign jurisdiction [Source 21]. Despite a high E-Government Development Index (EGDI) ranking, internal challenges such as agency silos and a lack of coordinated digital sovereignty strategies hamper the development of a unified national response to these dependencies [Source 16] [Source 20].

4.1 Cloud Infrastructure and Market Dynamics

The Swedish cloud hosting market mirrors broader European trends, characterized by the overwhelming dominance of non-European hyperscalers. United States providers control approximately 72% of the European cloud market, while local European providers hold a shrinking share of roughly 13% [Source 12]. This market asymmetry presents a risk of "digital colony" status, where critical national infrastructure relies entirely on foreign technology stacks that are subject to external geopolitical and legal pressures [Source 17].

Local infrastructure is robust but heavily interconnected with global networks. Netnod operates the largest Internet Exchange Point (IXP) in the Nordics, and the Stockholm Internet eXchange (STHIX) serves as a secondary critical hub [Source 15]. However, the routing of traffic remains opaque; while high-capacity local exchange points exist, there is no definitive data quantifying the percentage of domestic traffic that remains strictly within Swedish borders versus traffic routed internationally [Source 15].

The disparity in Research and Development (R&D) spending and infrastructure investment between U.S. hyperscalers and local providers has created a "feature gap." Swedish organizations often prefer foreign providers for their advanced AI/ML capabilities and global reach, despite the sovereignty risks [Source 12] [Source 17]. Consequently, Swedish entities seeking sovereign hosting solutions face a trade-off between regulatory compliance and technical capability.

4.2 Legal Framework and Jurisdictional Risks

Sweden's data localization landscape is defined by the conflict between EU privacy laws and U.S. surveillance authorities. The invalidation of the EU-US Privacy Shield (Schrems II) and the instability of the subsequent EU-US Data Privacy Framework create a volatile legal environment for data transfers [Source 13].

Key Legal Challenges: * **Extraterritoriality:** The U.S. CLOUD Act allows U.S. law enforcement to compel American tech companies to disclose data stored on servers in Sweden. This creates a "jurisdictional backdoor" that undermines the concept of data residency [Source 13] [Source 17]. * **Regulatory Enforcement:** The Swedish Data Protection Authority (IMY) maintains a strict stance. Notably, it has previously ruled that the use of tools like Google Analytics constitutes an unlawful transfer of personal data, signaling that mere residency of data in Sweden is insufficient if the provider is subject to U.S. law [Source 13]. * **Compliance Burden:** New EU directives, including NIS2 (cybersecurity) and DORA (digital operational resilience), impose strict requirements on essential entities to maintain control over their supply chains. This exacerbates the challenge of using foreign hyperscalers, as regulated sectors must demonstrate multi-vendor survivability and exit strategies [Source 17].

Unlike some nations that have enacted explicit data localization laws (e.g., Russia, China, Indonesia), Sweden relies on the GDPR framework to restrict data flows. There are no specific Swedish statutes mandating localization for broad categories of data, but the legal risks associated with transfer effectively force localization for sensitive citizen information [Source 14].

4.3 Public Sector and E-Government Sovereignty

Sweden consistently ranks highly in digital governance, placing sixth globally in the 2020 UN E-Government Survey [Source 16]. However, the hosting of sensitive citizen data—such as healthcare records, tax information, and national IDs—remains a critical vulnerability.

The public sector is currently experiencing a "cloud deadlock." Agencies are hesitant to migrate sensitive workloads to the public cloud due to the risk of unlawful disclosure under the Public Access to Information and Secrecy Act if U.S. authorities access the data [Source 21]. This risk aversion is compounded by a lack of "sovereign cloud" definitions; while U.S. providers offer "sovereign" products, these often fail to fully mitigate the risk of extraterritorial access [Source 17].

Structurally, Sweden's approach to digital sovereignty is fragmented. An OECD review identified significant obstacles, including a silo-based approach among government agencies, weak coordination powers, and a lack of clear leadership in the digital agenda [Source 20]. This fragmentation makes it difficult for the government to negotiate effectively with hyperscalers or to develop a cohesive national private cloud alternative. Mitigation strategies currently focus on building legal expertise within agencies to negotiate complex contracts and exploring "sovereign solutions" that attempt to insulate data from foreign laws, though the efficacy of these solutions remains unverified [Source 21].

4.4 Domain Name Ecosystem (.se)

The national top-level domain, .se, remains a critical component of Sweden's local digital identity. It is the preferred choice for entities conducting business within the country and for content-driven sites such as news portals and blogs [Source 5].

Historically, the .se domain saw restrictive registration rules until liberalization in 2003, which led to a surge in adoption. Today, it is viewed as a trusted marker for local presence, distinct from generic TLDs like .com or .org [Source 5]. However, the domain ecosystem is not immune to broader legal trends; 2024 saw an increase in domain name case filings for .se, indicating growing contention and commercial activity within the namespace [Source 5]. While specific consumer trust metrics are unavailable, the continued preference for .se suggests it functions as a de facto localization marker for Swedish consumers.

References

- [Source 1] Help us pick another future data center location : r/ProtonMail - Reddit (https://www.reddit.com/r/ProtonMail/comments/14dee9e/help_us_pick_another_future_data_cente
- [Source 5] The .SE domain extension now 65% cheaper. New registration rules ... (https://blog.resellerspanel.com/domain-names/dot-se-domain-names-now-cheaper.html)
- [Source 12] 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 13] Norwegian DPA warns against EU-US data transfers - Piwik PRO (https://piwik.pro/blog/norwegian-dpa-warns-against-eu-us-data-transfers/)
- [Source 14] The Nature, Evolution and Potential Implications of Data ... - OECD (https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/11/the-nature-

evolution-and-potential-implications-of-data-localisation-measures_249df37e/179f718a-en.pdf)

- [Source 15] Join the largest IX in Northern Europe - Netnod (https://www.netnod.se/ix)
- [Source 16] 2020 United Nations E-Government Survey (https://www.un.org/en/desa/2020-united-nations-e-government-survey)
- [Source 17] Digital Sovereignty of Europe: Choosing the EU Cloud Provider (https://gartsolutions.com/digital-sovereignty-of-europe/)
- [Source 20] Digital Government Review of Sweden (EN) - OECD (https://www.oecd.org/content/dam/oec government-review-of-sweden_7917ba3f/4daf932b-en.pdf)
- [Source 21] Mitigating the risk of US surveillance for public sector services in the ... (https://policyreview.info/articles/analysis/mitigating-risk-us-surveillance-public-sector-services-cloud)

Chapter 5

Security

Executive Summary

Sweden maintains a sophisticated digital infrastructure characterized by a high degree of network centralization and a generally robust security posture, though specific vulnerabilities in routing security persist. Intelligence indicates that Sweden maintains a "Final Cyber Safety Score" above 89, positioning it as a resilient actor in the global cyber domain `[Source 1]`. However, the national network topology exhibits significant "chokepoint" vulnerabilities, particularly regarding reliance on single upstream providers like TWELVE99 Arelion Sweden AB, which supports a vast number of downstream networks `[IYP-GRAPH]`. While the majority of critical Autonomous Systems (ASNs) have implemented Resource Public Key Infrastructure (RPKI) validation to mitigate routing attacks, notable exceptions among top-tier providers create potential vectors for route hijacking and instability `[IYP-GRAPH]`. Historical data confirms Sweden's susceptibility to global campaigns, such as the WannaCry ransomware incident which impacted local authorities `[Source 2]`.

5.1 Network Topology and Infrastructure Vulnerabilities

The structural integrity of Sweden's internet architecture is defined by a high concentration of dependency on a limited number of backbone providers. Analysis of the network topology identifies TWELVE99 Arelion Sweden AB as a critical systemic vulnerability; it functions as a massive chokepoint with 165,954 other ASNs depending on it for connectivity `[IYP-GRAPH]`. This extreme centralization presents a substantial strategic risk, as a successful large-scale Distributed Denial of Service (DDoS) attack against this single entity could cascade through the global routing table, severing connectivity for a significant portion of dependent networks.

Secondary chokepoints include GlobalConnect AB (2,988 dependencies) and AS-VULTR (1,289 dependencies). Furthermore, dependency analysis reveals that direct downstream clients of key Swedish ASNs, including Telia Company AB and Bahnhof AB, often exhibit a 100% dependency score, indicating a lack of redundancy and high susceptibility to upstream service disruptions

[IYP-GRAPH].

5.2 Routing Security and RPKI Implementation

The implementation of routing security measures, specifically Resource Public Key Infrastructure (RPKI) Route Origin Validation (ROV), is inconsistent across Sweden's critical network nodes.

Critical ASN Status: * **Validated:** The two most significant domestic chokepoints after the major backbones—ASN 20473 (1,289 dependencies) and ASN 13335 (956 dependencies)—have successfully implemented "Validating RPKI ROV" status. This suggests a proactive defense posture against BGP hijacking for these specific networks [IYP-GRAPH]. * **Vulnerable:** A significant security gap exists within ASN 12552. Despite being the third most significant domestic chokepoint with 747 dependencies, it is currently classified as "Not Validating RPKI ROV" [IYP-GRAPH].

Broader Adoption Issues: Intelligence identifies a list of Swedish ASNs that have failed to implement basic RPKI filtering. This list includes entities such as A3IT-AS, ADMAX Admax AB, ADMINOR Adminor Aktiebolag, and ADVANIA-AS Advania Sverige AB [IYP-GRAPH]. The failure of these entities to validate routing information increases the national attack surface, allowing for the potential propagation of illegitimate routing announcements.

5.3 Threat Landscape and Incident History

While current specific metrics regarding real-time DDoS volume and duration targeting Sweden are not definitively quantified in open-source intelligence [Source 3], the country remains a target for broad-spectrum cyber threats. Historical precedence for widespread disruption exists; Sweden was among the nations impacted by the massive WannaCry ransomware infection, which successfully compromised systems within local government authorities [Source 2].

Current assessments of Sweden's cyber safety rely on composite indices. Sweden maintains a "Final Cyber Safety Score" exceeding 89, reflecting a strong baseline capability in cyber defense, despite the topological and routing vulnerabilities identified in the physical and logical network layers [Source 1].

References

- [Source 1] Global Cybercrime Report 2024: Which Countries Face the Highest Risk (https://www.mixmode.ai/blog/global-cybercrime-report-2024-which-countries-face-the-highest-risk)
- [Source 2] Massive ransomware infection hits computers in 99 countries - BBC (https://www.bbc.com/news/technology-39901382)

- [Source 3] State of Application Security 2024 | Cloudflare (https://www.cloudflare.com/resources/assets/s
5907_State-of-App-Security-2024.pdf)
- [IYP-GRAPH] Internal Knowledge Graph (Network Topology and RPKI Status Data)

Chapter 6

Governance

Executive Summary

Sweden's digital governance framework is characterized by deep integration with European Union (EU) regulatory standards, prioritizing a model that balances innovation with fundamental rights. The nation's legal architecture for the digital domain is anchored by the General Data Protection Regulation (GDPR) and the Swedish Act on Electronic Commerce, ensuring strict data protection and consumer safeguards [Q7 Source 1][Q6 Source 1]. Unlike some global counterparts, Sweden exhibits no documented instances of state-mandated internet shutdowns or widespread blocking of social media platforms, reflecting a governance approach that favors open connectivity [Q5 Source 1].

However, a notable strategic gap exists in Sweden's international legal interoperability regarding cybercrime; intelligence indicates that as of June 2023, Sweden had not ratified the Budapest Convention on Cybercrime [Q2 Source 1]. This absence potentially limits specific procedural powers and streamlined mutual legal assistance mechanisms available to treaty parties. Current strategic trends suggest Sweden is pursuing a "trust and excellence" model, particularly regarding Artificial Intelligence (AI), aiming to foster industrial capacity while maintaining democratic values, rather than adopting a strictly control-oriented surveillance model [Q12 Source 1].

6.1 Legal Framework for Digital Rights and Data Privacy

Sweden's data privacy regime is fully harmonized with the EU's General Data Protection Regulation (GDPR), which serves as the primary enforcement mechanism for personal data handling. Organizations operating within Sweden are subject to strict collection, processing, and storage protocols. Enforcement is overseen by the national Data Protection Authority, which retains the power to levy administrative fines of up to €20 million or 4% of a company's total worldwide annual turnover for non-compliance [Q7 Source 1][Q7 Source 3].

Regarding freedom of speech in the digital domain, Sweden operates under the framework of the EU Digital Services Act (DSA). The DSA mandates due diligence and transparency from social media companies regarding illegal content [Q11 Source 2]. Intelligence suggests that the implementation of these regulations has created a complex environment for content moderation. There are indications that platforms may be engaging in the over-removal of legally permissible content to mitigate regulatory risks, raising concerns about the stifling of legitimate discourse [Q11 Source 1]. Despite these moderation challenges, there are no specific national laws granting the Swedish government broad, arbitrary powers to restrict online political or social discourse [Q10 Source 1].

6.2 Cybercrime and International Cooperation

A critical assessment of Sweden's stance on international cybercrime cooperation reveals a divergence from the standard European framework. As of mid-2023, Sweden was not listed among the 68 parties that have ratified the Budapest Convention on Cybercrime [Q2 Source 1]. Non-ratification implies that Sweden does not automatically benefit from the Convention's specific procedural tools, such as expedited preservation of stored computer data, production orders, and the 24/7 network for immediate assistance in investigations [Q2 Source 1].

Despite this, Sweden's domestic legislation is influenced by the standards set by the Convention, and the country engages in broader international dialogues. Recent diplomatic activity includes engagement with the United Nations Convention against Cybercrime (adopted December 2024), which the United States has noted as a potential framework for global cooperation, provided it is implemented with domestic safeguards [Q9 Source 2].

6.3 Electronic Commerce and Telecommunications Regulation

The foundational legislation governing Sweden's digital economy is the **Swedish Act on Electronic Commerce and Other Information Society Services**. This Act implements EU Directive 2000/31/EC and establishes the liability standards for online service providers, including intermediary liability for illegal content hosted on their platforms [Q6 Source 1]. This legal structure is designed to facilitate cross-border trade and harmonize e-commerce rules, reducing barriers for digital goods and services [Q6 Source 1].

Telecommunications regulation is overseen by the Swedish Post and Telecom Authority (PTS). The regulatory framework is derived from the Electronic Communications Act and EU directives, which generally favor general authorizations over individual licensing to promote market competition [Q1 Source 2][Q8 Source 1]. While the EU framework aims to reduce political discretion in licensing, global trends indicate that spectrum allocation processes can remain susceptible to complexity and incumbent advantages [Q8 Source 1].

6.4 Strategic Governance Outlook

Sweden's governance trajectory is currently defined by a regulatory model focused on "enabling innovation and rights" rather than centralized control. This approach aligns with the EU's strategy to promote “trustworthy AI,” aiming to boost research and industrial competitiveness while safeguarding fundamental rights [Q12 Source 1].

This innovation-centric model is evident in the public sector’s digital transformation strategies, which emphasize the use of digital technologies to improve efficiency and governance effectiveness [Q12 Source 4]. However, the drive for transformation faces challenges regarding the speed of technological advancement and the need to balance risk-taking with traditional administrative control mechanisms [Q12 Source 3].

References

- [Q1 Source 2] The Swedish Post and Telecom Authority’s Spectrum Policy - PTS (https://www.pts.se/contentassets/d5ec269637ff4f5586213c4cdbf668a1/pts-spectrum-policy.pdf)
- [Q2 Source 1] Budapest Convention on Cybercrime: (https://www.pgaction.org/pdf/2023/2023-07-06-presentation-by-mr-kralik-council-of-europe.pdf)
- [Q5 Source 1] Internet shutdowns cost countries $2.4 billion last year (https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf)
- [Q6 Source 1] Digital Business Laws and Regulations Report 2025-2026 Sweden (https://iclg.com/practice-areas/digital-business-laws-and-regulations/sweden)
- [Q7 Source 1] GDPR Countries in 2026 | GDPR Advisor - GDPR Consultant (https://www.gdpradvisor.co.uk/gdpr-countries)
- [Q7 Source 3] Sweden GPDR & Consumer Protection Law Guide | Pocketlaw (https://pocketlaw.com/content-hub/the-consumer-protection-s-equivalent-to-the-gdpr-is-introduced-in-sweden)
- [Q8 Source 1] Telecommunications Regulation Handbook - ITU (https://www.itu.int/ITU-D/treg/Documentation/Infodev_handbook/2_Licensing.pdf)
- [Q9 Source 2] Explanation of Position of the United States on the Adoption of the ... (https://usun.usmission.gov/explanation-of-position-of-the-united-states-on-the-adoption-of-the-resolution-on-the-un-convention-against-cybercrime-in-ungas-third-committee/)
- [Q10 Source 1] europe’s decade-long campaign to censor the global (https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/2026-02/THE-FOREIGN-CENSORSHIP-THREAT-PART-II-2-3-26.pdf)
- [Q11 Source 1] Online content moderation - Current challenges in detecting hate ... (https://fra.europa.eu/en/publication/2023/online-content-moderation)
- [Q11 Source 2] Preventing “Torrents of Hate” or Stifling Free Expression Online? (https://futurefreespeech.org/preventing-torrents-of-hate-or-stifling-free-expression-online/)
- [Q12 Source 1] European approach to artificial intelligence (https://digital-strategy.ec.europa.eu/en/polici
approach-artificial-intelligence)
- [Q12 Source 3] Interview Johan Magnusson | UOC (https://www.uoc.edu/en/news/2025/interview-johan-magnusson)

- [Q12 Source 4] Digital Government Strategies for Transforming Public Services in … (https://www.oecd.org/content/dam/oecd/en/publications/reports/2016/07/digital-government-strategies-for-transforming-public-services-in-the-welfare-areas_b4c29161/0d2eff45-en.pdf)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 7

Strategic Synthesis & Roadmap

Chapter 8

Section 7: Strategic Synthesis & Roadmap

To: The Office of the Prime Minister / The President **From:** Chief Strategy Officer **Date:** October 26, 2025 **Subject:** STATE OF THE DIGITAL NATION – DIAGNOSIS AND ACTION PLAN

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

The Narrative: The Glass Fortress Sweden stands as a global paradox. We are a "Glass Fortress"—technologically advanced and transparent, yet structurally fragile. We possess the envy of Europe in physical access (99.9% 5G, Top 3 in Fiber) and a population that is digitally native. However, our digital sovereignty is an illusion. We rely on American hyperscalers to host our government's brain (Cloud dependency) and route our traffic through a highly centralized, insecure "chokepoint" architecture that is vulnerable to hybrid warfare.

The Strategic Paradox: "Robust Access, Fragile Routing" While we have successfully hardened our physical borders (NATO integration) and physical cables (Baltic surveillance), we have neglected the *logical* layer of our territory. * **The Contradiction:** We spend billions defending the Baltic Sea cables from Russian sabotage, yet we allow our domestic internet traffic to be routed through unvalidated pathways (lack of RPKI) that a foreign adversary could hijack without ever deploying a ship. We are locking the front door while leaving the digital windows wide open.

8.2 2. SWOT Analysis: The Strategic Cheat Sheet

STRENGTHS (Internal)	WEAKNESSES (Internal)
World-Class Connectivity: 99.9% 5G coverage and deep fiber penetration provide a massive economic engine. **Arctic Advantage:** Northern Sweden (Kiruna/Boden) offers green energy and cooling, ideal for AI/HPC dominance. **Trusted Brand:** The `.se` domain and Swedish privacy laws are viewed globally as markers of integrity.	**The "Stockholm Chokepoint":** IXPs are heavily centralized in the capital. A kinetic or cyber strike on Stockholm isolates the nation. **Routing Hygiene:** Critical ASNs (including government suppliers) fail to validate routes (RPKI), inviting traffic hijacking. **"Cloud Deadlock":** Public sector paralysis due to conflict between Swedish secrecy laws and US CLOUD Act extraterritoriality.

OPPORTUNITIES (External)	THREATS (External)
Green AI Superpower: Position the Arctic region not just as a mining hub, but as the "Green GPU" capital of Europe for AI training.	**Hybrid Warfare:** Adversaries (Russia) targeting Baltic subsea cables to sever connectivity with the continent.
Nordic Cloud Consortium: Leverage Nordic cooperation to build a sovereign "GovCloud" that rivals US hyperscalers in compliance, if not scale.	**Digital Vassalage:** Total reliance on US tech stacks (AWS/Azure) renders Swedish data subject to US surveillance laws.
Nearshoring: Attracting EU sensitive data storage that requires GDPR compliance + physical safety.	**BGP Hijacking:** State-sponsored routing attacks targeting the "TWELVE99 Arelion" dependency to blackout Swedish connectivity.

8.3 3. Strategic Roadmap: The Policy Agenda

8.3.1 Phase 1: Immediate - "Hardening the Logic" (Months 1-6)

- **Objective:** Close the invisible security gaps that cost nothing but political will.
- **Action 1 (The "RPKI Mandate"):** Issue an executive decree that **no government agency** may sign a contract with an ISP or Cloud Provider that does not fully implement RPKI Route Origin Validation.
  - *Why:* This neutralizes the threat of BGP hijacking targeting our critical "chokepoint" providers (like TWELVE99 Arelion) without needing new hardware.
- **Action 2 (Ratify Budapest):** Immediately ratify the Budapest Convention on Cybercrime.
  - *Why:* We are currently fighting cybercrime with one hand tied behind our back. We need the expedited international evidence-sharing tools this treaty provides.

- **Action 3 (The "Stockholm Redundancy" Audit):** Order a stress test simulating a total outage of Stockholm IXPs (Netnod/STHIX). Identify immediate rerouting capabilities to Northern hubs.

8.3.2 Phase 2: Medium Term - "Sovereign Infrastructure" (Months 6-24)

- **Objective:** Break the "Cloud Deadlock" and decentralize the physical network.
- **Action 1 (Arctic Digital Shield):** Incentivize the creation of a secondary, geo-redundant Internet Exchange Point (IXP) in the Luleå/Boden region.
  - *Why:* If Stockholm goes dark, the North must stay online to maintain government continuity and military communications.
- **Action 2 (The "Sovereign Cloud" Initiative):** Public-Private Partnership (PPP) to build a GDPR-compliant "GovCloud" using the existing green data centers in the North.
  - *Why:* Swedish tax data and health records cannot legally or strategically reside on infrastructure subject to the US CLOUD Act. We must offer agencies a viable, legal alternative to AWS/Azure.
- **Action 3 (Cable Diversity):** Subsidize new subsea cable routes that do *not* follow the standard Baltic paths (e.g., direct links to Norway/UK/North America) to reduce reliance on the vulnerable Baltic Sea bed.

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

- **Objective:** Export the "Swedish Model" of secure, green digitalization.
- **Action 1 (Green AI Diplomacy):** Position Sweden as the EU's "AI Training Ground." Market our low-latency, green-energy compute capacity to EU nations seeking to meet climate goals while training Large Language Models.
- **Action 2 (Nordic Digital Fortress):** Formalize a "Nordic Digital Defense Pact" combining the networks of Sweden, Finland, and Norway into a single, interoperable mesh that can survive the isolation of any single member state.

8.4 4. Final Verdict

8.4.1 Investability Score: HIGH

Explanation: Despite the security nuances, Sweden remains a premier destination for capital. The fundamentals—energy, connectivity, and stability—are unmatched. The risks identified (routing security, cloud dependency) are solvable governance issues, not structural failures. Investors in AI infrastructure and Green Tech will find no better soil in Europe.

8.4.2 Maturity Score: MATURE (With Specific Vulnerabilities)

Explanation: Sweden is not "developing"; it is fully arrived. However, it suffers from "Complacency of the Competent." We have built a Ferrari (the infrastructure) but left the keys on the dashboard (routing security). The next phase is not about *building* more, but *securing* what we have built against a hostile geopolitical reality.