STRATEGIC COUNTRY REPORT: SWITZERLAND

Automated Strategic Analyst (v2.2 Parallel)

12 February 2026

Contents

Chapter 1

Geopolitics

Executive Summary

Switzerland's geopolitical posture is currently undergoing a significant recalibration, shifting from traditional rigid neutrality toward a more collaborative security stance in response to the Russian invasion of Ukraine. While maintaining its core diplomatic neutrality, the nation is actively exploring greater interoperability with NATO and neighboring states to bolster its security architecture [Source 1]. In the digital domain, Switzerland is firmly aligned with the European Digital Bloc due to geographic reality and physical infrastructure integration, yet it maintains a complex diplomatic balancing act by engaging with initiatives like China's Digital Silk Road [Source 4].

Domestically, the Swiss government has prioritized "Digital Sovereignty" to reduce external technical dependencies, adopting strategies that favor open-source software and hybrid multi-cloud environments [Source 2], [Source 3]. However, the nation's internet infrastructure exhibits signs of centralization. Analysis reveals a heavy reliance on a small cadre of upstream transit providers, specifically Swisscom and Liberty Global, the latter of which represents a significant connectivity chokepoint [Internal Graph]. This concentration creates potential resilience risks despite the country's advanced technological standing.

1.1 Geopolitical Standing and International Digital Role

Switzerland's geopolitical standing is defined by a re-evaluation of its historical neutrality. The security environment following the invasion of Ukraine has prompted the Swiss government to seek closer cooperation with like-minded nations and explore participation in NATO exercises, signaling a pivot toward Western security architectures while attempting to preserve its diplomatic autonomy [Source 1].

The country continues to leverage its status as a host nation for international organizations to influence global digital policy. The World Economic Forum (WEF) in Davos serves as a critical platform where Swiss leadership advocates for unity and partnership in addressing technological

challenges [Source 5]. Through these forums, Switzerland facilitates high-level dialogue on the evolving geopolitical landscape and digital governance, positioning itself as a neutral broker in an increasingly fragmented global digital economy [Source 5], [Source 6].

1.2 Digital Sovereignty and Strategic Autonomy

To counter the risks of foreign technical dependence, the Federal Council has adopted the "Switzerland's Digital Sovereignty Strategy." This framework defines digital sovereignty as the state's capacity to act and monitor its digital space independently [Source 2]. The strategy is overseen by an interdepartmental working group led by the Federal Department of Defence, Civil Protection and Sport, tasked with anticipating external risks and coordinating protective measures [Source 2].

Key pillars of this strategy include: * **Open Source Promotion:** Prioritizing open-source software to enhance innovation and reduce vendor lock-in [Source 2], [Source 7]. * **Hybrid Multi-Cloud Approach:** Utilizing diverse cloud providers to prevent reliance on single foreign entities [Source 2], [Source 7]. * **Trustworthy Infrastructure:** Developing state-controlled digital identities (e-ID) and secure data spaces [Source 2].

Despite these efforts to secure autonomy, Switzerland remains physically and digitally anchored to the **European Digital Bloc**. Its landlocked geography necessitates integration with European fiber networks. However, Switzerland has also positioned itself as a potential node for the Digital Silk Road (DSR) by signing a Memorandum of Understanding (MoU) with China regarding the Belt and Road Initiative. This creates a geopolitical duality: Switzerland is physically integrated with Europe but diplomatically open to acting as a transit point for Asian digital flows [Source 4].

1.3 Critical Infrastructure and Connectivity Risks

Switzerland's internet transit landscape is characterized by a high degree of centralization, which presents potential bottlenecks for national connectivity.

Transit Provider Concentration: Traffic analysis indicates a significant reliance on the top three upstream transit providers. **Swisscom (Schweiz) AG** leads with 4,415 incoming dependencies, followed by **Init7** (2,530) and **iFog GmbH** (2,076) [Internal Graph]. This centralization suggests that a disruption affecting Swisscom could have cascading effects across the national network.

Chokepoint Analysis: Further analysis of Autonomous System Numbers (ASNs) identifies critical dependencies. **Liberty Global B.V.** exhibits the highest "chokepoint score" (1611), indicating that a significant number of other ASNs rely on it for transit. **Cloudflare** (956) and **Swisscom** (883) also serve as critical transit nodes [Internal Graph]. The prominence of these entities highlights a structural vulnerability where specific commercial operators hold disproportionate influence over the country's international connectivity.

References

- [Source 1] Neutrality After the Russian Invasion of Ukraine - NDU Press (https://ndupress.ndu.edu/Media Article-View/Article/3511995/neutrality-after-the-russian-invasion-of-ukraine-the-example-of-switzerland-and/)
- [Source 2] Federal Council adopts report on Switzerland's digital sovereignty (https://www.news.admin.ch/en/newnsb/2VPWG78YrVs4eAVeiklQx)
- [Source 3] Swiss Federal Council adopts report outlining national approach to digital sovereignty (https://cadeproject.org/updates/swiss-federal-council-adopts-report-outlining-national-approach-to-digital-sovereignty/)
- [Source 4] Prefiguring China's digital silk road to Europe: Connecting Switzerland (https://munkschool.utoronto.ca/belt-road/research/prefiguring-chinas-digital-silk-road-europe-connecting-switzerland)
- [Source 5] Over 60 heads of state gathered at Davos 2026. Here's what they … (https://www.weforum.org/stories/2026/01/heads-of-state-gathering-davos-2026-what-they-saying/)
- [Source 6] Davos 2026: Special address by Mark Carney, PM of Canada (https://www.weforum.org/stories 2026-special-address-by-mark-carney-prime-minister-of-canada/)
- [Source 7] Digital sovereignty: How Switzerland can secure its digital … - ti&m AG (https://www.ti8m.com/en/blog/digitale-souveraenitaet-schweiz)
- [Internal Graph] Internal Knowledge Graph (IYP-GRAPH)

Chapter 2

Infrastructure

Executive Summary

Switzerland maintains a highly advanced telecommunications infrastructure characterized by exceptional mobile network coverage and a robust, albeit centralized, internet backbone. As of Q4 2024, Switzerland is one of only two European nations to exceed 80% 5G availability, having achieved over 90% population coverage as early as 2019 [Source 4][Source 5]. The national internet topology exhibits strong traffic localization, with key domestic operators actively participating in Internet Exchange Points (IXPs), thereby reducing latency and reliance on external transit for local traffic [IYP-GRAPH].

However, strategic vulnerabilities exist within the logical layer of the network. Analysis of Autonomous System Numbers (ASNs) reveals significant centralization, with GTT-BACKBONE serving as a critical dependency node for over 12,000 downstream relationships, representing a potential single point of failure or chokepoint [IYP-GRAPH]. While specific physical data center locations remain opaque in current intelligence, the logical infrastructure is supported by diverse fiber-optic operators including Swisscom, Green.ch, and Gas&Com [IYP-GRAPH]. Future capacity planning is active, with the Federal Communications Commission (ComCom) preparing for the next major mobile spectrum award scheduled for 2029 [Source 2].

Mobile Network Infrastructure & Spectrum

Switzerland has established itself as a leader in mobile network deployment within Europe. The country's aggressive rollout strategy resulted in over 90% 5G population coverage by the end of 2019 [Source 5]. This momentum has continued, with recent metrics indicating that Switzerland, alongside Denmark, stands as a regional outlier with 5G availability exceeding 80% as of late 2024 [Source 4].

Spectrum Allocation and Future Planning To sustain this capacity, regulatory bodies are actively managing spectrum resources. The Federal Communications Commission (ComCom) has instructed the Federal Office of Communications (OFCOM) to prepare for the reallocation of

mobile radio frequencies set to expire in 2029. A public tender, likely utilizing an auction format, is projected for 2026 to address potential frequency shortages [Source 2]. This planning occurs amidst global trends showing a historic low in spectrum prices in 2024, though the long-term decline in pricing during the 5G era may be stabilizing [Source 3]. The availability of low-band spectrum remains a critical factor for operators to maintain capacity and speeds, particularly as data-intensive technologies like Extended Reality (XR) emerge [Source 3].

Internet Backbone & Critical Dependencies

The Swiss internet backbone is defined by a mix of national incumbents and major international transit providers. Network analysis identifies specific ASNs that act as critical hubs, exhibiting disproportionately high downstream dependencies.

Network Centralization and Chokepoints GTT-BACKBONE (ASN 3257) appears as a primary structural chokepoint, managing 12,302 incoming dependencies. This high degree of centrality suggests that a significant portion of the Swiss network relies on this single entity for connectivity [IYP-GRAPH]. Other critical nodes include: * **COLT Technology Services (ASN 8220):** 1,858 incoming dependencies. * **Cloudflare (ASN 13335):** 956 incoming dependencies. * **Swisscom (ASN 3303):** The national incumbent retains a significant topological weight with 883 dependencies [IYP-GRAPH].

Internal analysis of `d.hege` scores reveals that several central ASNs have a score of 1.0, indicating 100% dependency for specific relationships. This signifies a lack of redundancy in certain segments of the network, creating potential vulnerabilities to targeted disruption or technical failure [IYP-GRAPH].

Interconnection & Traffic Localization

Switzerland exhibits a healthy ecosystem of traffic localization, driven by active participation in Internet Exchange Points (IXPs). The primary physical exchange point is located in Zurich (ZRH) [Source 1].

Peering Behavior Key national operators demonstrate high levels of IXP membership, which facilitates the direct exchange of traffic within national borders rather than routing through international transit. * **Swisscom (Schweiz) AG:** Reports 36 IXP memberships. * **WOODYNET-1:** Reports 38 IXP memberships. * **Switch (Academic/Research network):** Reports 28 IXP memberships. * **Global Tech Giants:** Microsoft and Google both maintain 28 IXP memberships within the Swiss jurisdiction [IYP-GRAPH].

This high density of peering relationships suggests a resilient logical topology for domestic communications, ensuring that local data traffic remains largely within the country, enhancing both speed and data sovereignty [IYP-GRAPH].

Fiber Optic Assets

While specific data regarding the urban-rural density of fiber deployment is unavailable, the network graph identifies several key entities holding fiber optic facilities. These include traditional telecommunications providers and specialized infrastructure firms. * **Init7 (Switzerland) Ltd:** Identified with 22 facilities. * **GAS&COM AG:** Identified with 19 facilities. * **LITECOM AG:** Identified with 9 facilities. * **GREEN (green.ch AG):** Identified with 6 facilities [IYP-GRAPH].

These assets form the physical backbone supporting the high-bandwidth requirements of the mobile and fixed-line networks described above.

References

- [Source 1] List of Internet exchange points - Wikipedia (https://en.wikipedia.org/wiki/List_of_Internet_
- [Source 2] Preparation for the next award of mobile telephony licences (https://www.news.admin.ch/en/ns
- [Source 3] Evolution of prices for mobile spectrum & possible explanations (https://www.econstor.eu/bitst Seoul-2024-paper-007.pdf)
- [Source 4] The Envy of Europe: Nordics Lead in 5G Availability and Network … (https://www.ookla.com/articles/nordics-5g-q1-2025)
- [Source 5] 5G networks deployment and "Critical IoT" - Faist Group (https://www.faistgroup.com/news/5 networks-critical-iot/)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 3

Market

Executive Summary

The Swiss telecommunications market is characterized by a mature, highly concentrated oligopoly dominated by the incumbent, Swisscom. As of late 2024, the market structure remains rigid, with the top three operators controlling nearly 99% of the mobile subscriber base. Despite Switzerland's reputation for high-quality infrastructure, current intelligence indicates a sector facing significant revenue pressure. Financial indicators reveal a trend of commoditization and stagnating Average Revenue Per User (ARPU), a challenge consistent with broader Western European markets.

Strategically, the market is stable but saturated. While specific data on domestic pricing and network latency is currently opaque, the financial health of major operators is under scrutiny, evidenced by credit rating downgrades for the market leader. The investment climate remains favorable for foreign capital, driven by a transparent regulatory framework and alignment with international security standards. However, future growth is likely to be driven by infrastructure consolidation and efficiency optimization rather than organic subscriber expansion.

3.1 Competitive Landscape and Market Structure

The Swiss mobile market exhibits a distinct tiered structure, effectively operating as a stable oligopoly. As of the end of 2024, the market is dominated by **Swisscom**, which holds a commanding subscriber market share of approximately 54% `[ComCom]`. This level of dominance by a single incumbent is significant compared to more fragmented European markets.

The primary challengers are **Sunrise**, with a market share of 26.5%, and **Salt**, holding 18% `[ComCom]`. Together, these three Mobile Network Operators (MNOs) account for 98.5% of the market. The remaining 1.5% is attributed to cable network operators (CATV) `[ComCom]`. This concentration suggests a high Herfindahl-Hirschman Index (HHI), indicating a market with high barriers to entry and limited competitive intensity regarding market share shifts `[ComCom]`.

While specific evidence of a "disruptor" operator actively driving down prices is absent in current reporting, the market dynamics mirror Canadian models where major players possess significant market power, potentially limiting aggressive price competition [Competition Bureau Canada].

3.2 Financial Performance and Revenue Trends

The economic health of the Swiss telecom sector is currently defined by pressure on revenues rather than aggressive profitability. Intelligence suggests that Swiss operators are not immune to the global trend of telecommunications commoditization.

Revenue Pressure: There is a discernible strain on financial performance for the market leader. S&P Global Ratings recently downgraded Swisscom AG from 'A' to 'A-', a move indicative of weakening financial risk profiles or increased susceptibility to adverse economic conditions [S&P Global].

ARPU and Commoditization: While specific Swiss ARPU figures are not publicly detailed, the market is subject to the same pressures observed in Western Europe, where mobile ARPU has seen negative growth (CAGR -1.3%) and fixed broadband revenue remains flat [PwC - Outlook]. The inability to significantly raise prices in a mature market means that revenue growth is often negated by inflation [PwC - Competition]. Consequently, the market is viewed as highly competitive regarding revenue retention, even if subscriber shares remain static [Analysys Mason].

3.3 Investment Climate and Strategic Outlook

Switzerland maintains a robust and attractive environment for foreign investment in the telecommunications sector, underpinned by legal stability and integration with global standards.

Regulatory Environment: The Swiss regulatory framework is characterized by openness to Foreign Direct Investment (FDI). Recent legislative updates, including the "Blockchain Act" and corporate law reforms, aim to modernize the investment landscape. Furthermore, national security regulations implemented in 2023 mandate strict adherence to international standards for critical equipment, ensuring that infrastructure is operated within secure data protection jurisdictions [State Dept].

Consolidation Trends: The Swiss market is influenced by broader European trends toward consolidation. To address the capital-intensive nature of fiber and 5G deployment, there is a shift toward "Netco" models—separating infrastructure ownership from service provision. This trend is driving Mergers and Acquisitions (M&A) activity across the continent as operators seek cost synergies and scale to support investments in AI and next-generation networks [KPMG], [PwC - M&A].

References

- [ComCom] Mobile market shares (https://www.comcom.admin.ch/en/market-share)
- [S&P Global] Swisscom AG Downgraded To 'A-' From 'A' Following (https://www.spglobal.com/ratings/p
/view/type/HTML/id/3308899)
- [PwC - Outlook] Perspectives from the Global Telecom Outlook 2024–2028 (https://www.pwc.com/gx/en/
outlook-perspectives.html)
- [PwC - Competition] The state of competition in telecoms (https://www.pwc.com/gx/en/industries/tmt/t
state-of-competition.html)
- [Analysys Mason] Switzerland telecoms market report (https://www.analysysmason.com/research/conten
reports/switzerland-country-report-rddc0/)
- [State Dept] 2023 Investment Climate Statements: Switzerland (https://www.state.gov/reports/2023-
investment-climate-statements/switzerland)
- [KPMG] M&A trends in tech, media, and telecom (https://kpmg.com/us/en/articles/mergers-
acquisitions-trends-tech-media-telecom.html)
- [PwC - M&A] Technology, Media and Telecommunications M&A 2024 outlook (https://www.pwc.ch/en/insights/strategy/m-and-a-trends-technology-media-and-telecommunications-2024-outlook.html)
- [Competition Bureau Canada] Telecom Notice of Consultation CRTC 2019-57 (https://competition-bureau.canada.ca/en/how-we-foster-competition/promotion-and-advocacy/regulatory-adviceinterventions-competition-bureau/telecom-notice-consultation-crtc-2019-57-further-comments-competition-bureau)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 4

Localization

Executive Summary

Switzerland's approach to data localization and digital sovereignty is currently defined by the tension between its traditional stance on neutrality and privacy, and the operational reality of reliance on foreign technology infrastructure. The cornerstone of this domain is the revised Federal Data Protection Act (revFADP), which entered into full force on September 1, 2023. This legislation aims to align Swiss standards with European Union regulations while maintaining a distinct legal framework that does not mandate a legal basis for all data processing operations, unlike the GDPR [Source 1].

However, significant strategic risks remain regarding the extraterritorial reach of foreign jurisdictions. Swiss entities face complex legal challenges when utilizing foreign cloud infrastructure, particularly regarding the implications of the US CLOUD Act, which creates potential conflicts with domestic privacy mandates [Source 1]. While Switzerland possesses a robust domestic internet exchange ecosystem (e.g., SwissIX, CIXP), the lack of granular data on local traffic routing versus international "tromboning" obscures the true extent of network sovereignty [Source 1][Source 4]. Consequently, mitigation strategies currently prioritize Transfer Impact Assessments (TIAs) and the recommendation to utilize local providers for sensitive data to ensure it remains under Swiss jurisdiction [Source 1][Source 2].

4.1 Legal Framework and Cross-Border Data Transfer

The regulatory environment for localization is governed by the revFADP. While sharing core principles with the GDPR—such as transparency, data minimization, and purpose limitation—the Swiss framework is distinct. Notably, it requires explicit consent primarily for high-risk profiling or the processing of sensitive data, rather than for all processing activities [Source 1].

Regarding cross-border data flows, the revFADP mandates that any data transferred outside Switzerland must be sent to countries that ensure an "adequate level of data protection." This adequacy requirement is the primary legal mechanism for controlling data residency. The frame-

work is designed to facilitate interoperability with the EU while protecting Swiss data subjects, yet it does not explicitly ban foreign storage provided adequacy standards are met [Source 1].

4.2 Jurisdictional Risks and Digital Sovereignty

The most acute challenge to Swiss localization is the conflict between national jurisdiction and the extraterritorial application of foreign laws. Swiss analysts have identified the US CLOUD Act as a significant vector of risk, as it allows US law enforcement to compel data disclosure from US-based technology companies regardless of where the data is physically stored [Source 1].

This creates a "conflicting jurisdictional" landscape for Swiss businesses and government entities using hyperscalers (e.g., AWS, Microsoft Azure, Google Cloud). Key challenges include: * **Ambiguity in Liability:** It is often unclear who bears the legal liability when data spans borders and conflicting laws apply [Source 1]. * **Vendor Lock-in:** Technical difficulties in migrating large datasets across providers create a dependency on foreign environments, complicating efforts to repatriate data to Swiss jurisdiction [Source 1]. * **Transparency Deficits:** Ascertaining the precise location of data processing and access points by foreign entities remains technically difficult, hindering compliance verification [Source 1].

To mitigate these risks, data protection authorities and experts recommend conducting rigorous Transfer Impact Assessments (TIAs) to evaluate third-country laws. For critical services that do not require global 24/7 availability, there is a strong recommendation to prioritize local providers to ensure data remains strictly under Swiss legal oversight [Source 1][Source 2].

4.3 Infrastructure and Network Localization

Switzerland maintains a foundational layer of network sovereignty through its Internet Exchange Points (IXPs), specifically SwissIX and CIXP [Source 3][Source 5]. These exchanges are critical for keeping domestic traffic local. However, intelligence regarding the efficiency of this localization is limited; there is no definitive data available on the percentage of traffic exchanged locally versus traffic that is routed internationally ("tromboning") before returning to Switzerland. This intelligence gap is attributed to the fact that not all IXPs publish public traffic statistics [Source 1][Source 4].

In terms of hosting, major foreign hyperscalers such as Google Cloud and Microsoft Azure have established regions and zones, indicating a significant foreign presence in the Swiss hosting market [Source 1][Source 5]. However, specific market share data comparing these hyperscalers against local Swiss providers for government and enterprise sectors is currently unavailable, preventing a precise assessment of domestic infrastructure control [Source 2].

4.4 National Digital Identity

The adoption of the country code top-level domain (ccTLD) `.ch` serves as a proxy for national digital identity and localization. The `.ch` domain is the 14th largest ccTLD globally, suggesting a strong preference for a distinct national online presence among private individuals and companies operating within the region [Source 2][Source 3]. While specific percentages comparing `.ch` usage against generic top-level domains (gTLDs like `.com`) are not available, the prominence of the national domain indicates a foundational element of digital identity is in place, supporting the broader concept of digital sovereignty [Source 3].

References

- [Source 1] Unveiling the Swiss Data Protection Act (DPA) - BigID (https://bigid.com/blog/unveiling-the-swiss-data-protection-act-dpa/)
- [Source 2] DomainWire - centr.org (https://www.centr.org/content_page/download/8165/4618/41.html?r
- [Source 3] More than just .ch and .com: the huge variety of top-level domains (https://www.hostpoint.ch/en/blog/more-than-just-ch-and-com-the-huge-variety-of-top-level-domains/)
- [Source 4] IXP REPORT 2021 - Euro-IX (https://www.euro-ix.net/media/filer_public/35/73/3573f355-c90a-4b31-ae83-851b76cfa36b/ixp_report_2021.pdf)
- [Source 5] CIXP: Welcome (https://cixp.net/)
- [Source 1] Global Locations - Regions & Zones - Google Cloud (https://cloud.google.com/about/locations)
- [Source 2] Is AWS losing ground to Azure? : r/ValueInvesting - Reddit (https://www.reddit.com/r/ValueI
- [Source 1] Cloud Data Sovereignty Governance and Risk Implications of Cross … (https://www.isaca.org/resources/news-and-trends/industry-news/2024/cloud-data-sovereignty-governance-and-risk-implications-of-cross-border-cloud-storage)
- [Source 2] Sovereign Cloud And Data Sovereignty: An Overview – - Exoscale (https://www.exoscale.com/blog/data-sovereignty/)
- [Source 1] New Standard Contractual Clauses - Questions and Answers overview (https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en)
- [Source 2] Switzerland: Data Protection Officers Impose Broad Cloud Ban for … (https://news.ycombinator.com/item?id=46077885)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 5

Security

Executive Summary

Switzerland exhibits a mixed security posture characterized by robust routing security protocols but stagnating adoption rates for domain name system security extensions. Intelligence indicates that approximately 63.84% of Swiss prefixes are covered by valid Route Origin Authorizations (ROAs), suggesting a proactive approach to preventing route hijacking [1]. However, the deployment of DNS Security Extensions (DNSSEC) has encountered structural headwinds, with the national registry expecting a slowdown in growth due to market saturation among domestic registrars and a lack of incentives for foreign entities [2].

While the National Cyber Security Index (NCSI) indicates that Switzerland's profile was updated as recently as August 2025, confirming active governance monitoring [4], specific granular data regarding the prevalence of botnet nodes, DDoS attack volumes, and definitive global rankings remains unavailable in open-source reporting [5][6]. Consequently, the assessment of the Swiss cyber environment relies heavily on infrastructure configuration metrics rather than incident volume statistics.

5.1 Network Infrastructure and Routing Security

The resilience of Switzerland's internet infrastructure is primarily measured through its adoption of Resource Public Key Infrastructure (RPKI), a critical protocol for preventing Border Gateway Protocol (BGP) hijacking.

RPKI Adoption and Validation Current technical assessments indicate that 63.84% of IP prefixes originating from Switzerland are validated via RPKI [1]. This metric represents the percentage of prefixes covered by valid Route Origin Authorizations (ROAs), providing a significant buffer against accidental or malicious route leaks. While this demonstrates a relatively high level of maturity in routing security, the remaining unvalidated address space constitutes a "Not Found" status, leaving a portion of the network theoretically vulnerable to route manipulation [1].

BGP Dependency and Chokepoints Intelligence regarding specific BGP chokepoints—Autonomous Systems (ASNs) that act as critical gateways with high dependency—is currently inconclusive. Methodologies exist to map country-level topology and identify "Gateway ASs," but recent analysis has not definitively identified specific Swiss ASNs that exhibit a high degree of dependency from other national ASNs to the extent that they constitute confirmed systemic risks for hijacking or disruption [7].

5.2 Domain Name System (DNS) Security

The security of the .ch country-code Top-Level Domain (ccTLD) is managed by the SWITCH registry. Recent reporting highlights a plateau in the adoption of security extensions necessary to authenticate DNS data.

DNSSEC Implementation Challenges Reports from the .ch registry (SWITCH) for 2023 and 2024 indicate that while DNSSEC adoption was previously a priority, growth is expected to slow significantly [2][3]. The primary drivers for this stagnation include: * **Saturation:** Large Swiss registrars have already signed the majority of eligible domain names [2]. * **Foreign Registrar Incentives:** There is minimal business incentive for large foreign registrars to sign .ch domains, limiting the expansion of DNSSEC coverage outside of domestic providers [2]. * **Technical Limitations:** Registrars possess limited influence over signing processes when domain names utilize external name servers, creating a technical barrier to universal adoption [3].

5.3 Cyber Governance and Threat Landscape

Switzerland maintains an active posture in cyber governance, though specific comparative rankings and threat volume metrics are currently opaque.

National Cyber Security Index (NCSI) Switzerland's standing in the National Cyber Security Index is actively maintained, with the country's profile receiving updates as of August 2025 [4]. The NCSI evaluates the nation across 12 key areas, including legislation, cloud security, and crisis response, utilizing 49 measurable indicators [4].

Threat Intelligence Gaps Significant intelligence gaps exist regarding specific threat vectors within the Swiss digital borders: * **Botnets:** While global botnet operations, such as those involving Integrity Tech, are monitored, there is no definitive geographical breakdown identifying the percentage of infected machines or active botnet nodes specifically within Switzerland [5]. * **DDoS Activity:** Technical reporting on the volume and average duration of Distributed Denial of Service (DDoS) attacks targeting Swiss infrastructure is currently unavailable in open-source threat intelligence [6]. * **Global Rankings:** Recent reports from the International Telecommunication Union (ITU), including the Global Cybersecurity Index (GCI) 2024, do not explicitly list Switzerland's current ranking, preventing a direct trend analysis of its comparative global standing [8].

References

- [1] RPKI Presentation - LUNOG6 - RIPE NCC (https://www.ripe.net/documents/3171/RPKI_Presentat _LUNOG6.pdf)
- [2] Report 2024 of the registry for the ccTLDs .ch and .li (https://www.nic.ch/export/shared/.content/files
- [3] Report 2023 of the .ch Registry - NIC Liechtenstein (https://www.nic.ch/export/shared/.content/files/
- [4] National Cyber Security Index (NCSI) (https://ncsi.ega.ee/)
- [5] Sanctioning PRC Cyber Company Involved in Malicious Botnet Operations (https://china.usembassy-china.org.cn/sanctioning-prc-cyber-company-involved-in-malicious-botnet-operations/)
- [6] Internet Standards: IPv6 standard - an analysis of uptake in the EU (https://publications.jrc.ec.europa.
- [7] Autonomous System Choke Points In Country-Level Network Topology (https://apps.dtic.mil/sti/trecn
- [8] Global Cybersecurity Index 2024 - ITU (https://www.itu.int/en/ITU-D/Cybersecurity/Documents/G Cybersecurity-Index-E.pdf)

Chapter 6

Governance

Executive Summary

Switzerland maintains a sophisticated governance framework for its telecommunications and digital sectors, characterized by a strong legal separation between the regulatory authority and the executive branch. The Federal Communications Commission (ComCom) operates as the independent regulator, insulated from directives by the Federal Council, ensuring a non-political approach to market regulation [1] [2]. However, the current strategic landscape is defined by a growing tension between Switzerland's constitutional privacy guarantees and expanding state surveillance capabilities. While Article 13 of the Constitution protects privacy, recent and proposed legislative changes—specifically regarding the Ordinance on the Surveillance of Postal and Telecommunications Traffic (VÜPF)—grant authorities broad surveillance powers that may exceed those found in comparable US or EU jurisdictions [3] [4]. Furthermore, the enactment of the 2017 gambling law, which mandates ISP-level blocking of foreign websites, signals a shift toward a more interventionist digital policy, raising concerns regarding internet freedom and censorship [7]. Switzerland remains integrated into the international legal order regarding cybercrime through the ratification of the Budapest Convention [5].

6.1 Regulatory Independence and Structure

The governance of the Swiss telecommunications sector is anchored in the Law on Telecommunications (LTC) of 30 April 1997. This legal framework establishes the Federal Communications Commission (ComCom) as the primary independent regulatory authority. ComCom is comprised of seven independent specialists nominated by the Federal Council; crucially, however, the Commission is not subject to directives from the Federal Council or any other government department, ensuring operational autonomy [1] [2].

ComCom is responsible for high-level regulatory functions, including the granting of licenses, establishing access conditions, and approving supervisory measures or sanctions. The Federal Office of Communications (OFCOM) acts as the administrative arm, preparing business for

ComCom and implementing its decisions, but it does not hold independent decision-making power over market regulation [2].

6.2 Surveillance and Privacy Framework

Switzerland's surveillance apparatus is governed by a complex interplay between constitutional rights and evolving security legislation. Article 13 of the Swiss Constitution guarantees the right to privacy in telecommunications, and Article 36 stipulates that any restriction on these rights must have a legal basis, serve a public interest, and remain proportional [3].

Despite these safeguards, the legal environment is shifting toward expanded state access to data. The 2011 revision of the Swiss Criminal Procedure Code consolidated surveillance provisions, but more recent proposals regarding the Ordinance on the Surveillance of Postal and Telecommunications Traffic (VÜPF) suggest a significant widening of scope. Intelligence indicates that proposed revisions would require email and VPN providers to retain data for six months and log IP addresses. Furthermore, the proposed framework mandates that service providers must possess the capability to remove encryption (creating "backdoors"), although end-to-end encrypted messaging between users remains technically exempt [4]. These measures have drawn criticism for potentially creating a surveillance regime stricter than that of the United States or the European Union, potentially impacting Switzerland's status as a secure data haven [4].

6.3 Digital Rights and Content Regulation

The regulatory landscape for Internet Service Providers (ISPs) and digital content has moved toward increased restriction. A pivotal development was the enactment of the online gambling law on March 1, 2017. This legislation mandates that Swiss ISPs block access to foreign online gambling websites based on IP addresses or domain names. While the stated intent is revenue protection for licensed Swiss casinos, the mechanism has been criticized by civil society as a form of censorship that creates a precedent for "overblocking" and restricts the open internet [7].

There are no documented instances of the Swiss government blocking social media platforms [8]. However, legislative trends indicate a move toward stricter user identification. Proposed revisions to surveillance laws have been described as similar to the UK's Online Safety Act, potentially requiring identification for the use of various digital services, which would effectively eliminate anonymous usage [4] [9].

6.4 Data Protection and Emerging Technologies

The protection of personal data is governed by the Federal Act on Data Protection (FADP) [10]. In the realm of emerging technologies, Switzerland is pursuing a "proportionality approach" to regulation, particularly regarding Fintech and Artificial Intelligence (AI).

- **Artificial Intelligence:** Switzerland is in the process of ratifying the Council of Europe's AI Convention to align its domestic framework with international human rights and rule-of-law standards. A draft bill to implement these amendments is expected by late 2026 [11] [12].
- **Fintech and DLT:** The regulatory environment is designed to be enabling, featuring a "fintech license" and a sandbox regime to lower barriers to entry. The DLT Bill has provided legal certainty for distributed ledger technology assets, aiming to remove regulatory hurdles [13].
- **Cybersecurity:** The Information Security Act introduces mandatory reporting obligations for operators of critical infrastructure regarding cyber incidents, effective April 1, 2025 [12].

6.5 International Cooperation

Switzerland has ratified the Budapest Convention on Cybercrime, legally binding the nation to harmonized international standards. This ratification facilitates mutual legal assistance in electronic evidence gathering and the extradition of cybercriminals, signaling strong integration with Western legal norms for combating cyber offenses [5]. Switzerland is not a signatory to the African Union's Malabo Convention [14].

References

- [1] Organisation - Bakom (https://www.bakom.admin.ch/en/organisation-3)
- [2] Commissions - Bakom (https://www.bakom.admin.ch/en/commissions-2)
- [3] REFORMING SURVEILLANCE LAW: THE SWISS MODEL (https://btlj.org/data/articles2015/vol2 berkeley-tech-l-j-1261-1332.pdf)
- [4] Switzerland plans surveillance worse than US - Tuta (https://tuta.com/blog/switzerland-surveillance-plan)
- [5] UNTC - Budapest Convention (https://treaties.un.org/Pages/showDetails.aspx?objid=0800000280071
- [6] Civil society concerned about extensive data retention in Switzerland (https://edri.org/our-work/open-letter-civil-society-concerned-about-extensive-and-indiscriminate-data-retention-regime-in-switzerland/)
- [7] Switzerland: Blocking of gambling sites - gambling with human rights (https://edri.org/our-work/switzerland-blocking-gambling-sites-gambling-with-human-rights/)
- [8] Internet Shutdowns and the Limits of Law (https://ijoc.org/index.php/ijoc/article/download/13752/31
- [9] New surveillance & censorship law similar to the UK Online Safety (https://www.reddit.com/r/Switzerl
- [10] Data Protection Act, FADP - Federal law - Fedlex (https://www.fedlex.admin.ch/eli/cc/2022/491/en)
- [11] AI Watch: Global regulatory tracker - Switzerland | White & Case LLP (https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-switzerland)

- [12] AI, Machine Learning & Big Data Laws 2025 | Switzerland (https://www.globallegalinsights.com/prac areas/ai-machine-learning-and-big-data-laws-and-regulations/switzerland/)
- [13] Fintech Laws and Regulations 2025 | Switzerland (https://www.globallegalinsights.com/practice-areas/fintech-laws-and-regulations/switzerland/)
- [14] African Union Convention on Cyber Security and Personal Data (https://dig.watch/resource/african-union-convention-on-cyber-security-and-personal-data-protection-african-union)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 7

Strategic Synthesis & Roadmap

Chapter 8

Section 7: Strategic Synthesis & Roadmap

To: The President of the Swiss Confederation / Federal Council **From:** Office of the Chief Strategy Officer **Date:** October 26, 2025 **Subject:** National Digital Resilience & Sovereignty Assessment

---

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

The Narrative: The Fortress with a Single Gate Switzerland stands as a premier "Digital Fortress" in Europe. We possess world-leading 5G coverage, a legally robust data protection framework (revFADP), and a highly localized traffic ecosystem where domestic data rarely leaves our borders. We have successfully translated our historical diplomatic neutrality into a digital asset, hosting the world's most critical international organizations.

The Paradox: "Sovereign Policy, Dependent Pipes" Our strategic contradiction is acute. While our **policy** aggressively pursues "Digital Sovereignty" (reducing reliance on foreign software and clouds), our **physical and logical infrastructure** exhibits dangerous centralization. We are legislating for independence, yet our internet connectivity relies disproportionately on a specific commercial triad: **Swisscom, Liberty Global, and GTT-Backbone**. A technical failure or targeted attack on Liberty Global (a "chokepoint score" of 1611) or GTT could sever Switzerland's connection to the global internet, rendering our sovereign laws irrelevant. Furthermore, while we pivot politically toward NATO/EU security architectures, our data remains vulnerable to the extraterritorial reach of the US CLOUD Act via our reliance on American hyperscalers (AWS, Azure, Google).

8.2 2. SWOT Analysis: The Strategic Cheat Sheet

STRENGTHS (Internal)	WEAKNESSES (Internal)
Hyper-Connectivity: >80% 5G availability; global leader in mobile infrastructure.	**Critical Centralization:** Extreme reliance on 2-3 transit providers (Swisscom, Liberty Global, GTT) creates systemic fragility.
Traffic Sovereignty: Strong IXP ecosystem (SwissIX, CIXP) keeps local traffic within Swiss borders.	**Stagnant Hygiene:** DNSSEC adoption has plateaued; registrars lack incentives to secure domain names.
Regulatory Stability: Independent regulator (ComCom) and clear legal frameworks attract FDI.	**Revenue Squeeze:** Market saturation is compressing operator revenues (Swisscom downgrade), limiting capital for future redundancy.

OPPORTUNITIES (External)	THREATS (External)
The "Digital Geneva": Position Switzerland as the neutral hosting ground for sensitive global AI and diplomatic data.	**Jurisdictional Pierce:** US CLOUD Act allows foreign access to Swiss data hosted on US clouds, undermining privacy guarantees.
Nearshoring Hub: Attract EU tech firms seeking stability outside the EU regulatory bloc but with physical proximity.	**Geopolitical Squeeze:** Balancing the "Digital Silk Road" (China) with increased NATO/EU integration risks alienating both blocs.
Quantum-Safe Transition: Lead the world in upgrading banking/diplomatic networks to post-quantum encryption.	**Surveillance Overreach:** New domestic surveillance laws (VÜPF) threaten to erode the "privacy brand" that attracts investors.

8.3 3. Strategic Roadmap: The Policy Agenda

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

Objective: Secure the perimeter and patch the "Single Gate" vulnerability.

- **Action 1 (Infrastructure): Mandate Transit Diversity.** The Federal Council must issue a directive requiring all Critical Infrastructure sectors (Energy, Finance, Health) to audit their upstream providers. If they rely solely on Liberty Global or Swisscom, they must contract a secondary, distinct transit path immediately.
- **Action 2 (Security): Reignite DNSSEC.** The stagnation in domain security is unacceptable. Direct OFCOM to incentivize registrars to implement DNSSEC by default. Consider a "Security Tax Credit" for ISPs that achieve 90% validation rates.
- **Action 3 (Geopolitics): The "Data Residency" Audit.** Conduct a classified audit of government data stored on US Hyperscalers. Identify datasets vulnerable to the US

CLOUD Act and migrate them to strictly sovereign Swiss-owned clouds (e.g., Green.ch, Swisscom local centers).

8.3.2 Phase 2: Structural Reform (Years 1-3)

Objective: Resolve the paradox of sovereignty vs. dependence.

- **Action 1 (Market): Incentivize "Netco" Competition.** The market is an oligopoly. Rather than breaking up Swisscom, use subsidies to encourage alternative fiber backbones that physically bypass the Zurich-Geneva axis, creating a "Redundant Ring" through the Alps.
- **Action 2 (Governance): Clarify the Privacy/Surveillance Line.** The tension between Article 13 (Privacy) and VÜPF (Surveillance) confuses investors. Pass a "Digital Trust Act" that explicitly limits the scope of surveillance to serious crimes, reassuring the international banking and diplomatic community that Switzerland is not becoming a surveillance state.
- **Action 3 (Diplomacy): Define the "Digital Silk Road" Stance.** We cannot integrate with NATO cyber defense *and* be a node for China's Digital Silk Road without friction. We must choose: restrict Chinese hardware in the core network (following the UK/US model) to solidify our Western security alliance.

8.3.3 Phase 3: Vision & Leadership (Years 3-5+)

Objective: Establish Switzerland as the "Trust Anchor" of the AI Era.

- **Action 1 (Innovation): Sovereign AI Infrastructure.** Build a national high-performance computing cluster dedicated to training "Swiss-aligned AI" (neutral, privacy-preserving) to reduce dependence on Silicon Valley models.
- **Action 2 (Global Policy): The Davos Digital Accord.** Leverage the WEF to spearhead a global treaty on "Digital Neutrality" during wartime, ensuring that neutral nations' connectivity cannot be targeted by state actors.

8.4 4. Final Verdict

8.4.1 Investability Score: HIGH

- **Rationale:** Despite revenue pressures on operators, Switzerland remains a safe harbor. The legal framework is transparent, the physical grid is state-of-the-art, and the political stability is unmatched. It is expensive to operate here, but the premium buys certainty.

8.4.2 Maturity Score: MATURE (Bordering on Stagnant)

- **Rationale:** The infrastructure is built; the market is saturated. The challenge is no longer "growth" or "access," but **resilience** and **optimization**. We are not building a

network; we are defending a fortress. The stagnation in security protocols (DNSSEC) and the reliance on legacy incumbents are signs of a market that needs a strategic shock to innovate further.