Civil Society Input — Strategic Review of the National Cyberstrategy (NCS)

Topic 2: Digital Sovereignty in the Context of Switzerland's Cyber Resilience

Submitted by: ICT4Peace Foundation (civil society)
For: Consolidation by the civil-society representatives of the NCS Steering Committee
Date: July 2026

Recommendation: Yes. Digital sovereignty should be taken forward for inclusion in the NCS at the next revision — framed not as autarky or data localisation for its own sake, but as rights-based, resilience-oriented "open strategic autonomy": meaningful Swiss control over critical digital infrastructure, data and capabilities, achieved through diversification, transparency and openness rather than isolation.

1. Description of the topic

Digital sovereignty is the capacity of a state, its institutions, organizations and individuals to exercise meaningful control over the digital infrastructure, data, hardware and software on which they depend, and to reduce structural dependence on any single external provider or jurisdiction. In a cybersecurity frame, it is best understood as an enabler of resilience: the ability to maintain the confidentiality, integrity and availability of critical digital functions even under geopolitical pressure, supply-chain disruption or extraterritorial legal claims. It is multi-level — encompassing the sovereignty of the state and critical infrastructure, of organizations and also(including SMEs and NGOs), and of individuals over their own data — and multi-dimensional, combining protection, participation and the domestic provision of trustworthy alternatives. Crucially, sovereignty is not the opposite of openness: transparency, open standards and open-source solutions are among its strongest instruments.

2. Strategic relevance for Switzerland's cybersecurity governance and capabilities

- Switzerland's cyber resilience increasingly rests on infrastructure and services controlled by a small number of foreign, predominantly non-European, providers. This concentration creates systemic single points of failure and exposes critical data — including government, health and critical-infrastructure data — to extraterritorial access regimes such as the US CLOUD Act, under which providers may be compelled to disclose data regardless of where it is stored.
- The strategic environment has shifted: cloud and AI procurement decisions are now, in effect, geopolitical decisions. Reliance on foreign foundation models and platforms introduces dependencies that bear directly on national security and the continuity of essential services. In a world where access to advanced AI can be curtailed by foreign export controls or corporate decisions at short notice, developing robust, sovereign AI capabilities in Switzerland becomes a core security function — comparable to resilient energy or communications infrastructure — and a strategic industrial policy choice at the same time.

- **This is not hypothetical.** In June 2026, a US government export-control directive led Anthropic to disable access to its most advanced AI models for non US users, effectively overnight — the first export-control measure aimed at specific AI models. The episode is a vivid illustration of the danger of over-reliance on a handful of American providers: access to critical capabilities can be withdrawn at short notice by a single foreign jurisdiction, for reasons unrelated to the user, with no domestic recourse. The Canadian Prime Minister publicly cited the case as evidence of the strategic vulnerability such dependence creates.
- Switzerland has already begun to respond — the Swiss Government Cloud (migration planned from 2027 to 2031), the public "Souveräne Digitale Schweiz" initiative, and the fully open, Swiss-developed Apertus language model, with new updated versions scheduled to be released in summer 2026 (v.1.5) and at the end of 2026/beginning of 2027 (v.2.0)— but these efforts currently lack an explicit strategic anchor in the NCS. Naming digital sovereignty as a cyber-resilience objective would give coherence to measures that are today dispersed across separate policies.
- The topic maps directly onto existing NCS objectives — in particular "secure digital services and infrastructures", "empowerment", and the "leading role in international cooperation" — and can be addressed through adjustments to those objectives and measures rather than a wholly new pillar.

3. Specific relevance for civil society

- Civil society organisations — NGOs, human-rights defenders, journalists and the not-for-profit sector — are simultaneously among the most dependent on foreign digital platforms and among the most frequently targeted by cyber operations. Their operational security, and the safety of the vulnerable people whose data they hold, depends directly on where, and under whose control, that data sits.
- For individuals, digital sovereignty is inseparable from fundamental rights: control over one's own data (reinforced by the revised Federal Act on Data Protection, nFADP), privacy, and freedom of expression. Sovereignty measures must strengthen, not erode, these rights.
- Civil society also brings an essential caution: "sovereignty" can be invoked to justify surveillance, censorship, data-localization mandates or market fragmentation that harm rights and an open internet. A distinctively Swiss, civil-society-informed approach should ensure that sovereignty serves people and democratic resilience — not control for its own sake. This complements the perspectives of the economy (competitiveness, innovation, exit-ability) and academia (open research, talent), with which civil society's emphasis on rights and trust is fully compatible.

4. Assessment, arguments and recommendations

4.1 Civil society's target picture

A Switzerland that practices rights-based, open strategic autonomy: it retains meaningful control over the digital systems essential to its security and democracy, achieved through diversification, portability and transparency rather than isolation; it offers trustworthy domestic and open-source alternatives for sensitive workloads; it protects individuals' control over their data as a matter of fundamental rights; and it exercises sovereignty in a way that

is transparent, multistakeholder and rights-respecting, reinforcing rather than undermining an open, secure and interoperable internet, including the cloud and AI infrastructure on which public services, justice, health and economic activity increasingly depend.

4.2 Concrete proposals (at the level of NCS objectives and measures)

- **Under "secure digital services and infrastructures":** introduce a measure to assess and reduce critical digital dependencies — mapping concentration risk across cloud, software and AI supply chains; setting requirements for data confidentiality against extraterritorial access, data portability and provider exit-ability for sensitive workloads; and actively promoting sovereign and open-source options (e.g., the Swiss Government Cloud and Apertus) where appropriate.
- **Make sovereign AI a strategic priority:** treat sovereign large language models and associated infrastructure as top-tier critical capabilities; invest in strengthening Switzerland's open models such as Apertus so they are robust and trustworthy enough for sensitive public-sector and critical-infrastructure use; ensure procurement frameworks allow them to be chosen for such workloads; and recognise them explicitly as a driver of long-term economic competitiveness, research excellence and talent retention in Switzerland's AI ecosystem. The June 2026 suspension of foreign access to leading US models underlines why a credible domestic and open alternative is a matter of resilience, not merely industrial policy.
- **Under "empowerment":** build digital-sovereignty literacy among the public, SMEs and the non-profit sector, and support individuals' practical control over their personal data.
- **Under "leading role in international cooperation":** pursue open strategic autonomy in coordination with the EU and like-minded partners — prioritising interoperability and avoiding fragmentation — and use Switzerland's Geneva-based digital diplomacy to champion rights-based, multistakeholder norms for digital sovereignty.
- **Across all measures:** embed transparency and a human-rights impact assessment into sovereignty-related decisions, and ensure civil society is represented in their governance.

4.3 Expected benefits

Greater cyber resilience and continuity of essential services under geopolitical stress; reduced systemic exposure to single foreign providers and extraterritorial leverage; stronger protection of fundamental rights and of the data of vulnerable populations; increased public trust in Switzerland's digital infrastructure; opportunities for Swiss SMEs and the open-source ecosystem; and reinforcement of Switzerland's credibility and leadership, consistent with its neutrality and its role as host of International Geneva.

There is also a distinctive external dividend. By making sovereign LLMs a priority and hardening its own open models such as Apertus, Switzerland stands to gain twice over: greater resilience and autonomy at home, and a recognised position abroad as a trusted, neutral provider of open, rights-respecting AI beyond its borders. As recent events show other countries the cost of dependence on a few foreign providers, demand for credible, jurisdiction-neutral alternatives will grow — and Switzerland is unusually well placed, by reputation and values, to help meet it.

4.4 Potential consequences if not addressed adequately

Deepening structural dependence and exposure to geopolitical and legal leverage over critical and sensitive data; erosion of confidentiality for government, health and critical-infrastructure systems; disproportionate harm to civil society actors and the people they serve; loss of public trust; and the risk that the sovereignty agenda is shaped elsewhere — or captured by protectionist or surveillance-oriented framings — without Switzerland's rights-based, multistakeholder voice. Switzerland would also risk falling behind partners, notably the EU, that are already operationalising digital-sovereignty strategies.

ICT4Peace would welcome the opportunity to elaborate on any of these points, including at the Steering Committee meeting on 18 August 2026 if useful.

Selected references: Swiss National Cyberstrategy (NCS, 2023) and First Implementation Report (2025); Swiss Government Cloud (Federal Office of Information Technology, Systems and Telecommunication); Apertus open multilingual LLM (EPFL / ETH Zurich / CSCS, 2025); US export-control directive suspending foreign access to advanced Anthropic AI models (June 2026); revised Federal Act on Data Protection (nFADP).