Grant Agreement No.: 101135632 | **Call:** HORIZON-CL4-2023-DATA-01
Topic: HORIZON-CL4-2023-DATA-01-06 | **Type of action:** HORIZON-CSA

Nexus Forum SWOT analysis for the EU Computing Continuum (extended report)

A Comprehensive SWOT Assessment of Europe's Readiness for Distributed Edge-Cloud-IoT Technologies

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the other granting authorities. Neither the European Union nor the granting authority can be held responsible for them.

Copyright notice

Project funded by the European Commission in the Horizon Europe Programme		
Dissemination Level		
PU	*Public, fully open, e.g. web*	**x**
SEN	*Sensitive, limited under the conditions of the Grant Agreement*	
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

* *R: Document, report (excluding the periodic and final reports)*
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.
DATA: Data sets, microdata, etc
DMP: Data management plan
ETHICS: Deliverables related to ethics issues.
SECURITY: Deliverables related to security issues
OTHER: Software, technical diagram, algorithms, models, etc.

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

Executive summary

The Computing Continuum, understood as an integrated architecture distributing computation across edge devices, local processing nodes and cloud centres, represents a foundational technology shift with profound implications for European competitiveness, digital sovereignty and economic growth. Europe possesses significant strengths for continuum development: world-leading research capabilities, a robust regulatory framework focused on data protection and ethical governance, sophisticated federated infrastructure initiatives, and strategic commitment to technological sovereignty. However, Europe faces critical weaknesses that constrain leveraging these strengths: fragmentation across competing national and institutional initiatives, limited SME integration into large-scale programmes, insufficient capital markets and talent development mechanisms, energy cost disadvantages and dependence on non-European technology providers in critical domains.

This strategic analysis examines six foundational factors determining European continuum readiness: (1) Technology, Innovation and Research Capabilities, (2) Framework Conditions (regulatory and governance), (3) Enabling Conditions (open-source, standards, skills), (4) Infrastructures and Connectivity, (5) Collaboration and Engagement, and (6) Industry Participation. Each factor is analysed through a comprehensive SWOT framework identifying strengths to leverage, weaknesses to address, opportunities to pursue and threats to mitigate.

The SWOT analysis reveals 14 critical gaps that must be addressed to transform Europe's fragmented strengths into competitive advantage. These gaps span technological sovereignty, infrastructure fragmentation, regulatory complexity for SMEs, confidence in European solutions, cross-border data sharing, open-source sustainability, SME dependence on foreign providers, energy costs, quantum-HPC integration, initiative coordination, global participation, financing mechanisms, vendor lock-in risks, and semiconductor supply chains. Each gap represents a systemic barrier preventing Europe's considerable technological and regulatory assets from combining into a unified continental strategy. Closing these gaps is not optional; it is the prerequisite for realising continuum leadership.

The analysis reveals that Europe's path to computing continuum leadership does not require replicating US or China models but rather developing distinctive capabilities aligned with European values: federated rather than monopolistic infrastructure, open-source rather than proprietary platforms, values-based governance rather than a surveillance-oriented one, and distributed innovation rather than concentrated control.

Funded by the European Union

Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

Table of contents

Funded by the European Union

Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

Funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

1 Introduction

The European Cognitive Computing Continuum represents a strategic response to the accelerating convergence of edge computing, cloud infrastructures, and Internet of things (IoT) technologies. For Europe, achieving technological sovereignty and market leadership in this emerging domain is not merely a matter of technological ambition; it is essential for preserving digital independence, protecting critical data and infrastructures, and maintaining the capacity to shape global standards and norms around trusted, secure and human-centred digital systems.

The **NexusForum.EU** initiative was launched to analyse Europe's readiness to consolidate and lead the Cognitive Computing Continuum. This document presents the results of a comprehensive SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis conducted across six critical factors that collectively determine Europe's capacity to succeed in this space. While this report does not yet prescribe specific policy measures, future recommendations derived from this analysis are intended to be developed in alignment with the Strategic Destinations for Europe’s AI Computing Continuum Ecosystem, ensuring consistency with the broader vision for Europe’s AI, computing infrastructure and digital sovereignty.

The analysis integrates evidence from strategic policy reports, technical assessments and consultation with industry experts, researchers and policymakers across the EU. Rather than considering the continuum as a single technological challenge, this analysis disaggregates the problem into distinct but interconnected dimensions, from technological capabilities and regulatory frameworks to enabling infrastructure, industry engagement and international collaboration, each of which requires targeted yet coordinated action.

The primary purpose of this SWOT analysis is twofold: first, to provide European policymakers and strategic actors with a rigorous, evidence-based assessment of the current state of play and the critical dependencies and gaps that must be addressed; and second, to establish the analytical foundation for concrete policy recommendations and investment priorities that can accelerate Europe's transition toward a consolidated, competitive and sovereign Cognitive Computing Continuum.

The following sections present the detailed SWOT findings by factor, identify cross-cutting patterns and dependencies, and point toward the policy and strategic choices that will define Europe’s trajectory in this critical domain.

Funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

2 The methodological framework

2.1 Understanding the SWOT framework and its strategic value in NexusForum

A SWOT analysis is a structured strategic assessment tool that examines four interrelated dimensions: **Strengths** (internal positive factors), **Weaknesses** (internal limiting factors), **Opportunities** (external positive factors), and **Threats** (external negative factors). This framework is particularly valuable for policy analysis because it enables decision-makers to:

- Identify current capabilities and assets that can serve as foundations for future strategy
- Recognise structural limitations that require targeted intervention or mitigation
- Detect emerging possibilities that aligned investments or regulatory reforms could activate
- Anticipate external risks that demand proactive rather than reactive responses
- Align policy instruments (regulation, financing, coordination) with both internal capacity and external context

For the consolidation of the European Cognitive Computing Continuum, a SWOT framework provides a rigorous yet accessible methodology for translating complex technological and policy landscapes into actionable intelligence for decision-making at the European level.

2.2 Methodological rationale: the six factors

The European Union's capacity to achieve technological sovereignty and consolidate an integrated Edge–Cloud–IoT continuum depends on multiple interrelated dimensions. Rather than examining computing continuum deployment as a monolithic challenge, this analysis disaggregates it into six strategic factors, each addressing a distinct but interconnected policy and capability domain. These factors are analysed in detail to develop policy recommendations that promote the convergence of edge, cloud and IoT technologies and strengthen the EU's digital sovereignty and competitiveness in digital technologies.

- **Factor 1: Technology, Innovation and Research Capabilities** forms the technological foundation of the European Cognitive Computing Continuum. It encompasses R&D capacity, infrastructure maturity, semiconductor and manufacturing capabilities, and the broader innovation ecosystem. European technological capabilities relevant to the development of the continuum include both existing assets and the ability to respond to emerging research and innovation challenges.

  Analysing this factor aims at identifying current gaps between research challenges and technological capabilities in the European Cognitive Computing Continuum, thereby informing where additional effort, coordination or investment is needed. Parameters considered include prioritised research lines, current and future technological capacities, synergies with industry actors in R&D&I, and complementarities with strategic agendas in partner countries such as Japan and the Republic of Korea.

- **Factor 2: Framework Conditions** addresses the regulatory, strategic and institutional environment within which the computing continuum evolves. It covers EU policies and regulations (such as the Data Act, AI Act, CRA, DSA, DMA, SRIP and SWIPO), Member State coordination mechanisms, and the alignment of national strategies with EU-level objectives. These framework conditions constitute the boundary context (policies, strategies, plans and regulations) that either enable or constrain the deployment of continuum technologies.

The objective for this factor is to identify gaps that must be addressed to establish a coherent regulatory and policy context for the continuum. Parameters analysed include the main legal instruments, certification schemes such as EUCS+ and the Cloud Rulebook, government policies (e.g. subsidies and tax incentives), and national or regional strategies for infrastructure, research and innovation and strategic alliances.

- **Factor 3: Enabling Conditions** focuses on the cross-cutting prerequisites that facilitate the successful development, implementation and adoption of continuum technologies at scale. This includes open-source software and hardware ecosystems, adherence to open and interoperable standards, workforce skills and training, and ethical and societal aspects such as data protection, cybersecurity, transparency and equity.
- The objective of this factor is to identify all crucial topics that play a significant role in the development of Europe's Cognitive Computing Continuum. Parameters examined include skills and knowledge (for both the current workforce and future generations), training needs for different age groups, the role of open source, the promotion of standards and compatibility, and the ethical and social implications of continuum deployment.
- **Factor 4: Infrastructures and Connectivity** encompasses the physical and logical layers that underpin continuum operation: data centre networks, 5G/6G connectivity, terrestrial and space-based infrastructure, data platforms and backbone networks. This factor addresses the "where" and "how" of computing continuum deployment.

  Its objective is to improve open strategic autonomy in critical data infrastructures along the continuum and to identify infrastructure needs to enable a European single market for data, with sectoral data spaces and a trustworthy AI ecosystem. Parameters include digital infrastructure for edge and IoT, initiatives such as Collaborative Connected Computing Networks (3C Networks), questions of data ownership and sovereignty, data spaces and governance models, and the availability and quality of ICT services.
- **Factor 5: Collaboration and Engagement** examines mechanisms for coordination and alignment among European initiatives, between European and international actors, and across public–private partnerships. This factor addresses fragmentation and seeks to ensure that the computing continuum becomes a genuinely European endeavour rather than a collection of disconnected projects.

  The objective is twofold: first, to identify opportunities to ensure the alignment and active participation of EU companies directly involved in initiatives such as IPCEI-CIS and the European Alliance for Industrial Data, Edge and Cloud; and second, to identify opportunities to increase engagement at international level, especially with Japan and the Republic of Korea, and to evaluate possibilities for strategic alignment with relevant international initiatives. Parameters include international collaboration, strategies for digital autonomy, awareness and promotion of digital sovereignty, engagement mechanisms with international partners, strategic alignment with other initiatives, mobilisation of the European research and innovation ecosystem, and the development of win–win partnerships.
- **Factor 6: Industry Participation** focuses on the engagement, capacity and strategic alignment of European industry,from large technology and telecommunications companies to SMEs and startups. Industry participation is key to ensuring that policies and technological developments are translated into competitive products, services and market leadership.

  This factor aims to identify needs and barriers faced by industry in accessing necessary infrastructures and technologies in cloud and edge computing, and to ensure that policies and innovations are tailored not only to large companies but also to SMEs, which are vital for European digital sovereignty. Parameters include European market and industry

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

engagement, evidence from tools such as the European Data Market Monitoring Tool, links with initiatives like the European Alliance for Industrial Data, Edge and Cloud and IPCEI-CIS, and community-building and engagement activities designed to build on internal strengths and generate new external opportunities.

2.3 Data sources and analytical process

The SWOT analysis is grounded in a combination of extensive desk research and systematic review of strategic reports and policy documents, together with technical and market studies relevant to the Cognitive Computing Continuum. This includes, among others, high-level reports such as Mario Draghi’s “The Future of European Competitiveness” (2024) and Enrico Letta’s “Much More Than a Market: Speed, Security, Solidarity” (2024), European Commission digital strategies and work programmes, and research and innovation roadmaps in the areas of cloud, edge, IoT and AI. These sources provide the broader policy context, identify major technological and industrial trends, and inform the definition of the six factors and their parameters.

In parallel, the analysis incorporates feedback and contributions from stakeholders through targeted consultation processes. This includes a dedicated workshop held during the NexusForum.EU 2024 Summit in Brussels, which helped define the initial structure of the SWOT, as well as six thematic online working sessions conducted between January and March 2025, one per factor, involving project partners, industry representatives, researchers and policymakers.

The SWOT assessments were co-created in these sessions to reflect both technical expertise and strategic policy perspectives. The combination of evidence-based research and structured expert consultation ensures that the SWOT is both analytically robust and grounded in operational realities. A key outcome of this process is the identification of concrete gaps in the European Cognitive Computing Continuum, which will inform subsequent policy recommendations.

The SWOT assessments were co-created in these sessions to reflect both technical expertise and strategic policy perspectives. The combination of evidence-based research and structured expert consultation ensures that the SWOT is both analytically robust and grounded in operational realities. A key outcome of this process is the identification of concrete gaps in the European Cognitive Computing Continuum, which will inform subsequent policy recommendations.

The SWOT analysis presented in this document reflects the state of Europe's computing continuum landscape primarily as assessed during 2025; **given the rapid evolution of digital policy and computing technologies**, **some findings may require updating where significant developments have occurred since the analysis was completed.**

2.4 Structure and reading guide

The following section presents the SWOT analysis for each of the six factors. Each factor analysis includes:

1. **Introductory context**: A brief explanation of why this factor matters for the computing continuum and how it relates to European strategic objectives
2. **Strengths**: Internal capabilities and assets the EU can leverage

3. **Weaknesses**: Internal limitations or gaps requiring attention
4. **Opportunities**: External developments or policy reforms that could unlock competitive advantage
5. **Threats**: External risks demanding mitigation or proactive response
6. **Synthesis**: An integrative summary highlighting the factor's overall strategic position and its implications for policy

Interconnections and systemic logic

These six factors are not independent silos but interconnected dimensions of a single strategic challenge. For example, strong technological capabilities in Factor 1 without coherent framework conditions in Factor 2 risk remaining fragmented or underexploited; robust infrastructures in Factor 4 will not achieve their potential without enabling conditions in Factor 3 or active industry participation in Factor 6. The analysis of each factor reveals not only its internal strengths, weaknesses, opportunities and threats, but also dependencies and leverage points for cross-factor policy alignment, which are crucial for coherent and impactful EU-level interventions.

Funded by the European Union

Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

3 The SWOT analysis

3.1 SWOT Factor 1: Technology, Innovation and Research Capabilities

3.1.1 Context

Factor 1 constitutes the core technological pillar for consolidating the cognitive computing continuum in Europe. It encompasses the technological capabilities, innovation capacity, and research competencies that enable the EU to develop a sovereign, resilient, and globally competitive digital infrastructure.

Europe's position in this domain is characterized by a paradoxical yet potentially complementary landscape. On the one hand, the EU has solid strengths in advanced infrastructures, specialized telecommunications equipment suppliers, semiconductor manufacturing capabilities, and a strategically relevant aerospace sector. These elements form the foundation for a differentiated technological architecture centred on digital sovereignty and interoperability across heterogeneous and distributed systems.

However, these strengths coexist with structural weaknesses that limit their full exploitation. Slow adoption of advanced technologies in the European market, lack of trust in AI systems and data security, limitations in open-source technology capabilities, the loss of technology leaders to external markets, and insufficient R&D investment create a situation in which technical potential does not automatically translate into industrial leadership or market competitiveness.

At the same time, emerging opportunities, such as initiatives on semiconductor sovereignty, the development of federated technology ecosystems, the reorientation of research investment, and regulatory adaptation for advanced connectivity (e.g. 5G), provide concrete pathways to transform existing assets into sustainable competitive advantages. In parallel, external threats like demographic decline, brain drain, dependence on non-European actors, and aggressive strategies of global competitors require urgent and coordinated action to prevent the progressive erosion of Europe's technological capacity.

3.1.2 STRENGTHS

1. Diverse and Advanced Technological Infrastructure
Europe has built over decades a sophisticated and widely distributed computing infrastructure, comprising edge nodes, specialized data centres, and high-capacity interconnection networks. This diversity is the outcome of sustained public and private investment, rather than an accidental accumulation, and increasingly reflects a strategic orientation towards distributed and federated architectures suited to the computing continuum.

Initiatives such as Gaia-X play a central role in this context. Gaia-X is designed as a federated framework to guarantee digital sovereignty through interoperability among heterogeneous edge, cloud, and IoT service providers, allowing data and services to be shared under clear European rules. Complementary projects such as Structura-X (which aims to create a federated cloud infrastructure aligned with Gaia-X standards), SIMPL (facilitating interoperability and secure data access), and more recent initiatives such as Sovereign-X and

INFRA-X, consolidate an architecture capable of supporting complex computing continuum applications across sectors and borders.

In addition, the Important Project of Common European Interest on Next-Generation Cloud Infrastructure and Services (IPCEI-CIS) marks a significant step in Europe's commitment to developing competitive alternatives to hyperscaler platforms dominated by non-European actors. The planned IPCEIs on Artificial Intelligence and Cloud Infrastructures further reinforce a coherent trajectory of capability-building across critical layers of the computing continuum.

2. Robust European Telecommunications Equipment Suppliers

Europe hosts globally leading telecommunications equipment suppliers, notably Ericsson and Nokia, whose market presence and technological credibility constitute a strategic asset for the deployment of 5G, 6G and edge computing infrastructures. These companies are not merely hardware providers; they are active developers of frontier technologies in areas such as radio access networks, edge processing, network virtualisation, and distributed orchestration.

Their leadership is particularly relevant in a context of rising geopolitical tensions, where the availability of trusted suppliers becomes a key factor of national and European security. The presence of robust European vendors reduces dependency on non-European actors for critical network infrastructure and enables Member States and operators to base long-term cooperation on shared values, regulatory alignment and predictable governance. This underpins both strategic autonomy and the credibility of Europe as a secure technology provider.

3. Semiconductor Manufacturing Capabilities

Europe is home to ASML (Netherlands), the global leader in advanced lithography machines for semiconductor manufacturing. This position in the global value chain provides the EU with a unique technological and geopolitical asset: control over key production equipment that is indispensable for high-end chip fabrication.

This advantage is being reinforced by the European Chips Act, an ambitious initiative to strengthen Europe's competitiveness, resilience and sovereignty in semiconductor technologies and applications. At the same time, the growing adoption of open instruction set architectures such as RISC-V opens the possibility for European actors to develop their own chip designs without relying exclusively on proprietary architectures controlled by external players.

Semiconductors form the material substrate of the computing continuum. Without sufficient control and capacity in this layer, higher layers of infrastructure, software and applications remain exposed to supply disruptions and strategic dependencies. The combination of European strengths in manufacturing equipment, policy instruments like the Chips Act, and open architectures such as RISC-V creates a credible basis for a more autonomous and resilient semiconductor ecosystem.

4. European Aerospace Sector as a Transversal Innovation Engine

The European aerospace sector, with major actors such as Airbus, Thales and Leonardo, goes well beyond being a specialised niche market. It functions as a powerful driver of technological innovation, with effects that propagate transversally across the digital economy. Modern aerospace operations rely on sophisticated real-time data management, predictive analytics, distributed edge–cloud processing and large-scale IoT integration. Use cases such as predictive maintenance, route optimisation, satellite constellation management, and remote sensing data processing impose demanding requirements that push forward advances in cloud, edge and IoT technologies.

In this sense, the aerospace sector serves as a “living laboratory” where new computing continuum technologies can be developed, tested and validated under stringent reliability and security conditions before being generalised to other sectors. Aerospace actors are not only consumers of digital technologies, but also co-innovators contributing to the definition of performance, safety and interoperability standards. With the rapid development of space-based connectivity and low-Earth orbit constellations, the sector also offers a strategic opportunity to extend European digital sovereignty into space and to counterbalance the concentration of orbital infrastructures in the hands of a few global players.

3.1.3 WEAKNESSES

1. Slow Adoption and Deployment of Advanced Technologies

Despite possessing advanced technological capabilities and infrastructures, Europe faces a persistent gap between technical potential and actual deployment in the market. The uptake of cloud computing, edge solutions, IoT and advanced data analytics remains slower than required for global competitiveness, particularly among SMEs, traditional industrial sectors and regions with lower levels of digital maturity.

The underlying causes are multifaceted. From an economic perspective, many companies face uncertainty regarding the return on investment of digital transformation, are concerned about the total cost of ownership of cloud solutions or have had negative experiences with cost escalation. Culturally, a comparatively higher aversion to risk leads many European firms to wait for technologies to mature before adopting them. Furthermore, there is often limited access to dedicated financing for digitalisation, while public and private investment still prioritises traditional sectors over next-generation digital capabilities. The scarcity of visible “early adopters” and large-scale success stories further weakens the incentives for rapid diffusion.

2. Lack of Trust in AI Systems and Data Security

Although Europe benefits from robust data protection frameworks (such as the GDPR) and a strong base of secure data centre infrastructures, this does not automatically translate into operational trust in AI systems and advanced data-driven decision-making. There is pervasive uncertainty about how AI models are trained, how reliable their outputs are, and how responsibility is assigned when automated decisions produce harmful or biased outcomes. These concerns are particularly acute in high-impact domains such as health, finance, public administration and critical infrastructures.

In parallel, many organisations face issues related to data quality: data sources are often fragmented, incomplete or historically biased, which undermines the performance and fairness of AI systems. There is also a skills gap: while Europe has strong academic capabilities in AI research, many organisations lack multidisciplinary teams able to design, validate and maintain AI systems in production. The combination of technical opacity, quality concerns and limited in-house expertise fuels skepticism and slows down adoption, even when the regulatory framework is in principle favourable to trustworthy AI.

3. Limited Capabilities in Open-Source Technologies

Open-source software underpins a substantial share of today’s digital infrastructure, from operating systems and container orchestration to data platforms and AI frameworks. Yet Europe suffers from a shortage of teams with advanced capabilities to develop, maintain and evolve critical open-source components. This is a global challenge, but it tends to affect Europe more strongly given its fragmentation and the limited size of some national ecosystems.

The consequences are tangible. Key open-source projects on which European public administrations and companies depend may be maintained by small, overstretched teams with limited resources. Delays in security patches, lack of long-term maintenance and insufficient governance structures can directly affect the resilience of critical infrastructures. Moreover, the relative scarcity of large-scale European contributions to key open-source projects reduces Europe's influence over technical roadmaps and standards. This creates a vicious circle in which weak participation in open-source communities leads to weaker capabilities and greater dependence on external actors.

4. Brain Drain and Loss of Technology Leaders to External Markets
A significant number of Europe's most promising technology companies and entrepreneurs relocate part or all of their activities to other regions, especially the United States, or are acquired by non-European actors. This "brain drain" and externalisation of high-growth companies is a symptom of deeper structural issues in Europe's innovation and scaling environment.

Financing conditions are a central factor: venture capital markets in Europe are comparatively more conservative, with smaller ticket sizes and lower tolerance for high-risk, high-reward projects than in other major innovation hubs. Regulatory and market fragmentation also complicate scaling across borders, whereas competitors operate in larger, more homogeneous internal markets. The result is that European-origin companies often need to move abroad to access growth capital and global networks, leading to a loss of talent, intellectual property and strategic control over key technologies that were initially developed in Europe.

5. Insufficient and Fragmented R&D Investment
Investment in ICT research and development in Europe remains below the level required to sustain leadership in rapidly evolving technological domains. Public programmes such as Horizon Europe mobilise substantial resources, but funding is often dispersed across numerous calls and relatively small projects, with complex administrative requirements that can discourage participation by SMEs and emerging actors.

Furthermore, the translation of research results into industrial innovation is still uneven. High-quality research produced by European universities and research centres does not always find clear pathways to the market, due to gaps in technology transfer mechanisms, access to risk capital and the lack of long-term, mission-oriented programmes. Fragmentation across Member States, with overlapping national initiatives that are not always aligned, can dilute impact and reduce Europe's ability to compete at scale with more centralised innovation systems.

3.1.4 OPPORTUNITIES

1. Promoting Open Hardware Initiatives for European Semiconductor Sovereignty
The recent global chip shortages have underscored the vulnerability of relying on external semiconductor supply chains for critical sectors such as automotive, telecommunications, health and defence. At the same time, the emergence of open instruction set architectures such as RISC-V has broadened access to chip design capabilities and reduced barriers to entry for new players.

This creates a window of opportunity for Europe to accelerate investment in open hardware initiatives, combining industrial policy (e.g. the European Chips Act), support for design capabilities, and collaboration with industry and research organisations. By doing so, the EU can reduce its structural dependency on external suppliers, strengthen its position in key segments of the value chain, and build a semiconductor ecosystem aligned with European values and security requirements. A robust and more autonomous semiconductor base is indispensable for underpinning the entire computing continuum, from constrained edge devices to high-performance computing.

2. Developing a Federated Technology Ecosystem for Dispersed Resources

The global cloud market is currently dominated by a small number of hyperscalers that centralise data and computing capacity. Europe has an opportunity to promote an alternative model based on federated infrastructures and services, in which multiple providers remain independent but interoperable through common standards, reference architectures and governance frameworks.

Projects such as Gaia-X and IPCEI-CIS embody this approach by enabling edge, cloud and IoT nodes to share services, improve resource utilisation and offer users greater choice while preserving data sovereignty. A federated ecosystem can: bring computation closer to where data is generated; enable smaller providers and industrial players to participate in common platforms; reinforce compliance with EU rules on data protection, cybersecurity and competition; and enhance Europe's capacity to shape global norms on trusted and interoperable digital infrastructures.

3. Reorienting Research Investment and the Structure of Horizon Europe

The current configuration of EU research and innovation programmes, while extensive, often results in fragmented efforts and limited capacity to address large-scale, systemic challenges such as the consolidation of the computing continuum. There is an opportunity to adjust the design and implementation of programmes like Horizon Europe to enable more ambitious, mission-oriented initiatives.

A more strategic approach would involve concentrating resources on a smaller number of large, multi-country, multi-actor projects that explicitly target the development and deployment of end-to-end computing continuum solutions. Simplifying participation rules, especially for SMEs and emerging players, and providing longer-term, stable funding horizons would also increase the likelihood that research outputs translate into industrial capabilities and competitive products and services.

4. Clarifying Net Neutrality Rules for Innovative Use Cases Such as 5G Network Slicing

European net neutrality rules constitute an essential safeguard for an open and non-discriminatory internet. However, certain innovative technologies, particularly 5G network slicing and other forms of quality-differentiated services, require a regulatory framework that allows for technically justified differentiation while preventing anti-competitive practices and unfair discrimination.

Clarifying and updating guidance on how net neutrality applies to advanced connectivity use cases would enable operators and service providers to deploy network slicing and other innovative features in a legally certain environment. This would support new applications in areas such as connected and automated mobility, e-health, industrial automation and public safety, while preserving the core principles of openness, fairness and user rights that underpin the European regulatory model.

5. Coordinating Technical Standards at EU Level for Network APIs, Edge Computing and IoT

The fragmentation of technical standards and interfaces across national markets and vertical sectors remains a major barrier to the seamless deployment of computing continuum solutions in Europe. There is a clear opportunity to coordinate and align technical standards at EU level, particularly in areas such as network APIs, edge computing interfaces and IoT device interoperability.

By promoting common European reference frameworks and encouraging convergence around open, interoperable standards, the EU can reduce integration costs, accelerate deployment and make it easier for developers and service providers to scale solutions across borders and sectors. Coordinated standardisation efforts would also strengthen Europe's influence in international standard-setting bodies and help ensure that global norms reflect European requirements in terms of security, privacy, competition and sustainability.

6. Exploring Niche Markets: Aerospace and Telecommunications
In several mature digital markets, non-European actors have already consolidated dominant positions that are difficult to contest. Nevertheless, Europe retains significant strengths in specific strategic niches, notably aerospace and telecommunications, where it still has strong industrial players, advanced capabilities and a solid regulatory framework.

Leveraging these niches as launchpads for computing continuum solutions can generate multiple benefits. In aerospace, extending the continuum to include satellites and space-based services can provide secure connectivity, Earth observation and navigation services that are tightly integrated with terrestrial infrastructures. In telecommunications, the deployment of advanced 5G and future 6G networks, combined with edge and cloud capabilities, can support highly demanding industrial and public-sector use cases. These niches can serve as anchor markets that accelerate learning curves and support the emergence of competitive European solutions.

3.1.5 THREATS

1. Demographic Decline and Loss of Competitiveness
Europe is facing a structural demographic decline, characterised by ageing populations, low birth rates and, in some cases, net outward migration of younger cohorts. This trend directly affects the availability of skilled labour for technology-intensive sectors and constrains the capacity to renew and expand the digital workforce required by the computing continuum.

When contrasted with regions that enjoy more favourable demographic dynamics and larger young populations, Europe risks a relative reduction in its innovation and entrepreneurship base. This may limit the ability of European companies and research institutions to sustain the pace of technological change and compete effectively in global markets.

2. Brain Drain and Company Relocation
The ongoing loss of high-skilled professionals and high-potential companies to other regions exacerbates Europe's demographic challenges. When leading technology firms relocate or are acquired by non-European actors, not only are jobs and tax revenues affected, but entire innovation ecosystems are weakened, including supplier networks, research collaborations and startup communities.

Over time, this process can generate a self-reinforcing cycle in which the reduced presence of successful scale-ups and innovation leaders makes Europe less attractive for entrepreneurs, investors and talent, further accelerating the outflow of key actors. For the computing continuum, this implies that critical know-how, intellectual property and strategic decision-making may progressively shift outside the EU.

3. Global Competition and Strategic Dependencies
The EU operates in a global environment where a limited number of non-European actors dominate key technological layers, including cloud infrastructures, operating systems, key software platforms and advanced semiconductor manufacturing. These dominant positions are supported by coordinated industrial policies, large internal markets and deep pools of capital.

Such concentration creates strategic dependencies for Europe. In times of geopolitical tension or trade disputes, access to essential technologies, components or services could be restricted or become subject to conditions that do not align with European interests or values. Even in normal conditions, the asymmetry of bargaining power between European users and dominant external providers can limit Europe's ability to shape technical and contractual terms, reinforcing lock-in and limiting room for manoeuvre.

4. Dependence on Non-European Technologies if European Alternatives Are Not Sustained

Europe has launched several initiatives aimed at strengthening technological sovereignty including the Chips Act, Gaia-X, IPCEIs and various national programmes. However, there is a material risk that some of these initiatives may not reach sufficient scale, maturity or market adoption to constitute credible alternatives to non-European technologies.

If promising projects are not adequately funded, sustained over time and aligned across Member States, Europe may find itself in a situation where it has invested significant resources without achieving the intended autonomy, while external dependencies persist or deepen. This would weaken trust in public interventions, discourage private investment and reduce Europe's capacity to influence the evolution of key technologies in line with its strategic objectives.

5. Aggressive Strategies of International Competitors

Major international competitors, notably large US and Asian technology companies, deploy comprehensive strategies to expand their footprint in European markets and integrate European talent, data and infrastructures into their global ecosystems. These strategies combine acquisitions of European startups, large-scale infrastructure investments, intensive recruitment of local experts and strong engagement with public authorities and regulators.

While such investments can bring short-term benefits in terms of jobs and services, they can also contribute to the externalisation of strategic control, the erosion of local competitors and the concentration of data and intellectual property outside the EU. Over time, this may limit Europe's ability to autonomously define its technological trajectory, set its own standards and ensure that digital infrastructures and services evolve in line with European values and policy objectives.

3.1.6 SYNTHESIS

Factor 1 is characterised by a complex configuration in which solid structural strengths in infrastructure, semiconductor-related capabilities and strategic industrial sectors coexist with significant weaknesses in technology uptake, trust in emerging technologies, open-source participation, talent retention and the scale and coherence of R&D investment.

The EU has concrete opportunities to build technological sovereignty and competitiveness through open hardware and semiconductor initiatives, the development of federated infrastructures, the reorientation of research and innovation programmes, regulatory adaptation for advanced connectivity, the strategic use of strong niche sectors such as aerospace and telecommunications, and the coordination of technical standards at EU level. At the same time, threats related to demographic trends, brain drain, global competitive asymmetries, persistent dependencies and aggressive strategies of non-European actors underline the need for a sustained, coordinated and long-term response to ensure that Europe's technological potential is effectively translated into leadership across the computing continuum.

Funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

3.2 SWOT Factor 2: Framework Conditions

3.2.1 Context

Factor 2 addresses the regulatory, strategic and institutional environment that shapes the development and deployment of the Cognitive Computing Continuum across the EU. Framework conditions are the foundational layer of governance, encompassing EU policies and regulations, Member State coordination mechanisms, and the alignment of national strategies with European objectives, that either enable or constrain the mobilisation of technological capabilities and industry participation.

Europe's regulatory landscape in digital and technology policy is increasingly comprehensive and ambitious. Instruments such as the AI Act, Data Act, Digital Services Act, Digital Markets Act, Cybersecurity Act and Cyber Resilience Act represent the EU's commitment to establishing digital markets grounded in European values: fundamental rights protection, data privacy, fair competition, cybersecurity and sustainability. This regulatory ambition is a strategic asset, differentiating the EU in global markets and building trust among citizens and businesses. However, the complexity and fragmentation of this regulatory environment, where national implementations vary, compliance requirements overlap, and bureaucratic processes remain cumbersome, create significant operational friction.

The central challenge for framework conditions is to maintain Europe's regulatory leadership and values-based differentiation while simultaneously streamlining implementation, reducing administrative burden, and creating the unified market conditions necessary for European companies to scale and compete globally. This requires both consolidating existing regulations into more coherent frameworks and reforming institutional mechanisms to achieve faster, more agile policy-making. Without such alignment, Europe risks simultaneously over-regulating its own innovators while failing to create the market unity necessary to match the scale and competitive capacity of global competitors.

3.2.2 STRENGTHS

1. Europe as a Leader in Climate Policy and Digital Sustainability
Europe has established itself as a global leader in climate policy and environmental governance, with binding commitments to carbon neutrality by 2050 and the Green Deal framework. This leadership extends into digital policy, where the EU explicitly recognises the role of digital technologies in achieving climate and sustainability objectives. The Cognitive Computing Continuum, if properly architected, can become a critical enabler of European climate goals. Cloud, edge and IoT technologies, when deployed with sustainability as a design principle, can optimise resource utilisation, reduce energy waste, improve industrial efficiency and enable circular economy models across sectors.

The EU's regulatory framework increasingly mandates energy efficiency criteria for data centres and digital infrastructure, creating a differentiated competitive advantage. European computing continuum solutions can be marketed globally as inherently more sustainable and climate-conscious than alternatives from regions with less stringent environmental standards. This is not merely a compliance advantage; it is a market differentiation opportunity that allows

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

companies building sustainable computing solutions to compete on values and long-term risk reduction in global markets, a particularly important advantage as enterprises increasingly face shareholder and stakeholder pressure to reduce technology carbon footprints.

2. The AI Act as a Global Regulatory Gold Standard

The EU's AI Act represents the most comprehensive and sophisticated regulatory framework for artificial intelligence adopted by any major economic bloc. Rather than being purely restrictive, the Act balances innovation protections with rights protections by establishing a risk-based regulatory approach: high-risk AI systems face strict requirements, while lower-risk applications operate with minimal regulatory friction. This nuanced approach demonstrates that Europe can regulate innovation without strangling it.

The AI Act's promulgation as EU law, applicable to any organisation deploying AI in European markets, creates an extraterritorial regulatory effect. Global AI developers and service providers must increasingly adapt their systems to comply with the Act, effectively setting a global standard for trustworthy AI. The Act also includes provisions supporting SMEs and startups, recognising that regulatory burden must be calibrated to company size and capacity. Companies that design AI systems to meet the Act's standards gain access to European and globally-conscious markets while building trust with users and regulators worldwide, a particularly important advantage for the computing continuum, which increasingly incorporates AI-driven decision-making at the edge and cloud layers. The regulatory credibility this provides allows European companies to compete from a position of inherent compliance rather than post-hoc adaptation.

3. Codification of European Values in Digital Policy Framework

European Values, including data protection, personal privacy, cybersecurity, digital inclusion, environmental sustainability, and fundamental rights protection have been systematically embedded into digital policy instruments (GDPR, ePrivacy Directive, Data Act, AI Act, Digital Services Act). This represents a deliberate strategic choice to differentiate European digital governance from alternative models, creating a unified ethical and governance framework that simplifies decision-making for companies operating across Member States.

This values-based framework builds genuine trust with European citizens and businesses, encouraging uptake of digital services and reducing friction in data sharing arrangements. It also establishes a global normative position: when other countries adopt privacy and cybersecurity standards, they increasingly adopt European models, effectively expanding European influence. Digital inclusion provisions ensure that continuum technologies benefit entire populations, not just early adopters or wealthy regions. By transforming what could be regulatory burden into a market differentiator and governance legitimacy, companies and public administrations operating within this framework build trust with stakeholders and reduce the fragmentation that would otherwise result from inconsistent values frameworks.

4. Strong Data Sovereignty Framework and Infrastructure

Europe has established the world's most stringent data protection regime (GDPR) and is implementing sophisticated data sovereignty mechanisms through initiatives like Gaia-X. These create practical assurances that data generated and processed in Europe can remain under European control, subject to European law and European enforcement mechanisms. The existence of secure, Europe-based data centres certified under emerging standards (particularly Gaia-X "Label 3" certification, which requires physical server location in Europe and compliance with European values) provides the infrastructure necessary to implement data sovereignty commitments.

This framework is essential for the computing continuum because continuum architectures necessarily involve data flowing across multiple processing nodes, from edge devices to cloud centres. Without credible data sovereignty mechanisms, this distributed architecture creates

Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

data control vulnerabilities. Gaia-X and similar initiatives address this by establishing federated governance models where data remains under known jurisdictional control. Cross-border data flow mechanisms (such as those being developed with Japan and other partners) establish protected pathways for data transfer while maintaining sovereignty principles. Because data sovereignty addresses a genuine customer concern, the fear of data capture by non-European actors, it is not merely regulatory compliance but a genuine market demand. Companies in regulated sectors (finance, healthcare, government) increasingly require data sovereignty as a condition of technology adoption, creating a defensible market niche for European infrastructure and governance mechanisms meeting these requirements.

5. Digital Markets Act Creating Fair Competition and Ecosystem Opportunity
The Digital Markets Act (DMA) represents a strategic regulatory intervention designed to address the market concentration achieved by large non-European technology platforms (referred to as "gatekeepers": Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft). The DMA prevents these actors from leveraging their dominant positions to unfairly disadvantage competitors, requires data access and interoperability for competing services, and enables smaller actors to compete more effectively. For the computing continuum, the DMA prevents gatekeepers from using cloud or data centre dominance to foreclose competition in edge or IoT services and requires interoperability, preventing lock-in that would otherwise trap European companies in non-European technology stacks.

By creating a level playing field where performance and innovation capacity matter more than inherited advantages (first-mover scale, network effects, data lock-in), the DMA shifts competitive advantage toward European entrants who bring technical sophistication, regulatory compliance and values alignment. It creates space for European cloud service providers and edge-computing innovators to compete on merit rather than being disadvantaged by anti-competitive practices, enabling SMEs and startups to build viable business models without first-mover capture by dominant platforms. This effectively handicaps non-European competitors while empowering European ecosystem participants.

3.2.3 WEAKNESSES

1. Absence of a Unified EU Capital Markets Union
Despite decades of discussion, the EU lacks a true single, integrated financial market for equity and debt capital across Member States. This fragmentation creates a critical disadvantage for financing large-scale technology projects. European companies pursuing computing continuum technologies face fragmented access to venture capital, growth financing and project financing. A promising European computing company may secure seed funding in one Member State but struggle to find growth-stage capital without relocating to US markets.

In contrast, the US venture capital and private equity markets operate as a single, deep, liquid market where capital flows to the best opportunities regardless of geography. China's state-directed capital allocation mechanisms similarly ensure large-scale funding for strategic technology initiatives. The EU's fragmented approach means that even when European companies have superior technology or market positioning, they may lack adequate financing to scale production, build manufacturing capacity or fund market entry in competitive sectors. While regulatory excellence matters, execution requires capital; computing continuum infrastructure, data centres, edge facilities, network upgrades, requires multi-billion euro investments that cannot be adequately financed through fragmented national capital markets.

2. Insufficient Regulatory Compliance Monitoring and Enforcement
Europe has created an extensive regulatory framework for digital markets but lacks systematic, EU-level enforcement mechanisms to verify compliance and penalise violations. Where regulations exist but enforcement is weak, the rules effectively fail to constrain behaviour,

Funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

creating a situation where European companies face high compliance costs while non-European competitors operating in European markets may operate with minimal actual compliance burden. Fragmented national enforcement creates additional friction: a company compliant with regulations in one Member State may face compliance challenges in another.

This is particularly problematic for regulations like the GDPR, Data Act, and DMA, where enforcement should be consistent but in practice varies significantly by Member State. Weak enforcement also means that gatekeepers continue anti-competitive practices that regulations theoretically prohibit, because the actual penalty risk is low. Without robust, consistent enforcement, European companies gain no protection from regulatory compliance, and the burden of compliance falls disproportionately on those attempting good-faith compliance while competitors operating with minimal actual enforcement burden maintain competitive advantages.

3. Fragmented and Excessive Regulation Creating Market Fragmentation
Although the EU has created common regulatory instruments (AI Act, Data Act, DMA, DSA, CRA, etc.), implementation across Member States remains inconsistent. National regulators interpret rules differently, transposition into national law creates variations, and enforcement priorities differ. This creates a patchwork regulatory environment where a solution compliant in one Member State may face regulatory challenges in another. Additionally, some regulations overlap or create contradictory requirements, forcing businesses to navigate conflicting compliance obligations.

For computing continuum deployment specifically, this fragmentation is particularly damaging. A federated cloud or edge infrastructure operating across Member States must navigate multiple regulatory regimes simultaneously. Small and medium enterprises (SMEs) lack dedicated compliance teams and cannot absorb the cost of managing multiple regulatory frameworks, pushing them toward either operating in a single Member State and losing scale economies, or relocating to jurisdictions with simpler regulatory environments. Excessive regulation, regulations that impose compliance burdens disproportionate to actual risk or that duplicate other regulations, further compounds this problem by preventing the consolidation of European markets that is essential to the entire strategic vision of a "Digital Single Market". When regulations are fragmented or excessive, SMEs particularly cannot scale beyond their home market, reducing the pool of competitive European competitors and fragmenting computing continuum infrastructure itself.

4. Administrative and Bureaucratic Burden in Compliance and Funding Access
Compliance with digital regulations in Europe is administratively demanding. Regulations like the Cybersecurity Act and Cyber Resilience Act require formal assessments, periodic audits, vulnerability testing, documentation and reporting. For a startup or SME, these requirements demand significant organisational overhead, hiring compliance officers, implementing monitoring systems, maintaining documentation. The burden is not merely cost; it is distraction from core innovation activities.

Additionally, access to public funding for innovation (e.g., Horizon Europe grants, national innovation programmes) involves lengthy application processes, complex evaluation criteria, extensive documentation requirements and extended decision timelines. An innovator pursuing urgent market windows cannot afford to wait 12-18 months for a funding decision. The bureaucratic burden of funding access effectively locks out nimble, fast-moving innovators in favour of larger organisations with dedicated grant administration teams. Implementation of regulations also varies across Member States, requiring companies to understand and comply with different national procedures, timelines and interpretation practices. This creates additional compliance complexity for any actor operating cross-border. Since administrative and bureaucratic burden imposes costs that scale poorly for small organisations, while large, well-resourced companies can absorb compliance and funding-access complexity, it creates a

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

hidden tax on European innovation that particularly harms the ecosystem's capacity to generate new entrants and disruptive competitors.

5. Cyber Resilience Act Creating Unintended Barriers to Open Source
The Cyber Resilience Act (CRA), designed to improve cybersecurity of products and services, imposes requirements for vulnerability testing, audits, continuous support and security patching. These are reasonable requirements for commercial products. However, the CRA's application to open-source software, where development is often volunteer-driven, maintenance resources are limited, and commercial support models are nascent, creates unintended barriers that threaten the foundation of European digital infrastructure.

Open-source developers and maintainers now face formal compliance obligations they cannot reasonably meet without significant new resources. This creates two concerning outcomes: some open-source projects reduce activity or cease maintenance rather than incur compliance burden, directly harming the availability of critical infrastructure software; and only well-funded, commercially-backed open-source projects (like those backed by Red Hat, Canonical, or comparable companies) can achieve compliance, effectively commercialising open source and reducing community-driven innovation. This is particularly damaging for the computing continuum, which depends heavily on open-source software for edge computing, IoT platforms, containerisation, data processing and networking. Rather than strengthening cybersecurity, the regulation risks reducing the availability and diversity of security-critical software by creating regulatory barriers to precisely the category of software that underpins European digital infrastructure, despite treating open source as equivalent to commercial products despite their fundamentally different development and support models.

6. User Concerns About Lock-in, Data Control and Security
Despite Europe's strong data protection regulations, users, both individuals and organisations, harbour legitimate concerns about cloud and continuum technology adoption. Concerns include lock-in effects (difficulty switching cloud providers or extracting data); GDPR compliance burden (both for service providers and data subjects); cybersecurity risks from interconnected edge-cloud systems; and uncertainty about US cloud providers' obligations under the US Cloud Act (which requires US companies to disclose data to US government on request).

These concerns are not unfounded; they reflect real risks. They create friction in adoption of computing continuum technologies because organisations (particularly in regulated sectors) are uncertain whether adopting cloud or edge solutions will compromise data control or regulatory compliance. This hesitation slows market adoption and creates openings for non-European competitors to claim data sovereignty advantages. Until these concerns are addressed through concrete mechanisms such as workable data portability, transparent audit rights, practical lock-out prevention and verifiable data isolation, adoption will remain constrained, reflecting gaps between the regulatory promises of data protection and the lived experience of organisations attempting to operate within European regulatory frameworks while using cloud and continuum technologies.

3.2.4 OPPORTUNITIES

1. Reforming EU Regulation and Competition Stance for a Unified Digital Single Market
A strategic opportunity exists to accelerate completion of the Digital Single Market by harmonising telecommunications regulations across Member States and promoting consolidation and cross-border operations in digital infrastructure sectors. The current patchwork of national telecommunications regulations (frequency allocations, infrastructure requirements, operational permits) fragments what could be a unified market. Removing these barriers would enable pan-European telecommunications and cloud infrastructure companies to operate on equivalent terms across Member States, facilitating consolidation, combining

Funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

fragmented national operators into larger, more efficient entities capable of competing with global competitors.

This would accelerate infrastructure deployment (5G, 6G, fibre, edge computing facilities) by allowing operators to make investments based on European-scale economics rather than national silos. Specifically, harmonizing spectrum allocation, infrastructure sharing requirements, and cross-border interconnection standards would unlock billions in efficiency gains and accelerate computing continuum deployment. Regulatory harmonisation for a unified market converts regulatory fragmentation into market unity, which is particularly important for physical infrastructure (telecommunications networks, data centre facilities) where economies of scale are critical, since European-scale unified markets have historically outcompeted fragmented national markets.

2. Expanding the EU Chips Act to Accelerate European Semiconductor Capabilities

The EU Chips Act is a strategic industrial policy instrument aimed at increasing European semiconductor manufacturing capacity and reducing dependence on external suppliers. However, current funding levels and implementation timelines are insufficient to achieve the Act's strategic objectives. An opportunity exists to significantly expand the Act in terms of funding committed, scope of support and pace of implementation, including increased direct funding for new fabs (manufacturing facilities) in strategically important segments; accelerated public-private partnership models that share risk while enabling rapid deployment; and expanded support for chip design capabilities (particularly in advanced process nodes and specialised chips for edge computing and AI).

Given the geopolitical importance of semiconductors and the multi-year timescales required to build manufacturing capacity, ambitious public investment is strategically justified and necessary. Semiconductors are foundational to the computing continuum and to European technological sovereignty. Unlike many technology domains where Europe can innovate incrementally, semiconductor manufacturing requires multi-year, multi-billion euro commitments that cannot be made by individual companies or Member States and thus require EU-level strategic commitment and financing.

3. Implementing a Long-Term EU Quantum Computing Strategy

Quantum computing represents a frontier technology domain where Europe has research strength but lacks coordinated, large-scale investment strategy. An opportunity exists to establish a long-term, well-funded, coordinated quantum computing programme spanning research, technology development and industrial application, including harmonised funding architecture across Member States (avoiding duplication), coordinated research roadmaps, development of quantum-classical hybrid architectures, and pathways to quantum-secure cryptography.

Such a programme should be explicitly positioned as strategic autonomy investment: quantum computing capabilities will be essential for cryptography, optimisation and AI applications in the future computing continuum. Early leadership in quantum-continuum integration could give Europe significant competitive advantage. Importantly, this programme should have 20-30 year time horizons and explicit tolerance for long-term, high-risk research domains where public research funding is most appropriate. This allows Europe to invest deliberately in a frontier technology domain with centuries-long strategic importance. Unlike incremental improvements in existing technologies where Europe lags, quantum computing is still in foundational phases where current research choices can shape the entire trajectory, enabling coordinated European strategy to create unique advantage.

4. Dismantling Administrative and Regulatory Obstacles Through Regulatory Streamlining and Unified Authority Architecture

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

A strategic opportunity exists to fundamentally simplify Europe's regulatory architecture by consolidating overlapping regulations, creating a unified digital regulatory authority, and establishing clear, streamlined compliance pathways. This should include consolidation of overlapping regulations into coherent frameworks rather than layered regulation; creation of a single European Digital Authority with clear primary responsibility for digital markets, competition and cybersecurity; simplification of Horizon Europe and other public funding mechanisms to reduce application and compliance burden; and establishment of explicit SME-tailored compliance pathways with reduced burden for companies below certain thresholds.

Additionally, this opportunity includes lowering administrative burden for accessing public funding by streamlining grant application processes, accelerating decision timelines and reducing documentary requirements. Government programmes should be redesigned to support rapid deployment timelines consistent with technology market cycles (12-18 months for decision cycles, not 24-36 months). This converts a major weakness (administrative burden) into a competitive advantage, since Europe's underlying regulatory vision (values-based, citizen-centred, competition-enabling) is sound; the implementation is unnecessarily burdensome. Streamlined implementation would maintain regulatory intent while dramatically reducing operational friction, particularly for SMEs, and is low-risk because it does not require regulatory changes, only administrative redesign.

5. Removing Cross-Border Regulatory Barriers to Unified Digital Operations

An opportunity exists to establish truly reciprocal recognition of regulatory compliance across Member States where certification or compliance achieved in one Member State is automatically accepted in all others. This should include unified recognition of data protection compliance (organisations certified as GDPR-compliant in one Member State do not require recertification in others), unified recognition of cybersecurity certifications, unified recognition of AI Act compliance for high-risk systems, and unified spectrum and telecommunications licensing for cross-border infrastructure.

Additionally, establishing common frameworks for cross-border data flows, subject to data protection principles, would enable federated cloud and edge infrastructure to operate seamlessly across Member States. This directly enables the computing continuum's fundamental architecture, distributed, federated systems operating across national boundaries. Without reciprocal recognition, federated infrastructure must navigate 27 separate regulatory regimes, making it economically unviable. Reciprocal recognition converts fragmentation into unity while requiring only legal alignment (ensuring that all Member States' data protection implementations are genuinely equivalent) before establishing mechanisms that eliminate massive operational friction.

6. Scaling Digital Sovereignty Through IPCEI and Similar Large-Scale Strategic Initiatives

The Important Projects of Common European Interest (IPCEI) mechanism has proven effective at coordinating large-scale, multi-country, public-private initiatives in semiconductors (IPCEI-Semiconductors, IPCEI-Microelectronics) and cloud infrastructure (IPCEI-CIS). An opportunity exists to expand and deepen this model for computing continuum technologies, including additional IPCEIs explicitly targeting edge computing infrastructure, AI-specific cloud services, quantum computing, and secure communications systems; longer-term funding commitments (10-15 year timescales) that match technology development cycles; explicit mechanisms for technology transfer and capability building across participating companies; and mechanisms to ensure that IPCEI-developed technologies transition into sustainable commercial services.

IPCEIs are effective because they explicitly coordinate public and private investment, reduce duplication, align incentives, and create scale economies that individual Member States cannot achieve alone. Scaling digital sovereignty through IPCEIs leverages a proven institutional mechanism that has demonstrated success in other domains. The IPCEI model aligns public resources, private execution capacity and cross-border coordination, precisely the combination needed for large-scale continuum deployment, so expanding this model compounds its effectiveness.

7. Implementing EUCS+ Certification to Create Trusted, Competitive Cloud Infrastructure Market
The European Cybersecurity Certification Scheme for Cloud Services (EUCS+) is a EU-developed standard for cloud service security. An opportunity exists to systematically implement EUCS+ as the de facto standard for all cloud and edge infrastructure in Europe, with explicit government procurement preference and support mechanisms, including government commitment to procure only EUCS+-certified services; funding support to help cloud providers (particularly European SMEs) achieve EUCS+ certification; integration of EUCS+ into regulatory compliance frameworks so that certification counts as evidence of meeting cybersecurity requirements; and marketing support to communicate EUCS+ as a trust signal in global markets.

EUCS+ is effective because it is technically robust, developed by European cybersecurity expertise, and creates a unified standard that enables competition among providers rather than lock-in to any single vendor. Unlike proprietary security standards, EUCS+ is open and vendor-agnostic. This converts certification (a potential regulatory burden) into a market differentiator, allowing EUCS+-certified providers to compete globally on the signal of high security and European regulatory alignment. For European providers, EUCS+ certification is a competitive advantage; for non-European providers, achieving certification requires investment in alignment with European standards, creating friction.

3.2.5 THREATS

1. Innovation Constraints from Overly Strict AI and Emerging Technology Regulation
A significant threat exists that excessively strict regulatory requirements for AI and emerging technologies could slow European innovation below the pace required to compete globally. While the AI Act is generally well-designed, specific provisions, such as stringent requirements for high-risk AI systems, mandatory impact assessments, and proof-of-compliance burdens, could create such high barriers to entry that only well-resourced organisations can develop AI solutions. If regulatory requirements become stricter than those in other major markets, European AI research and commercial AI development could progressively migrate to less regulated jurisdictions.

This is particularly concerning for AI applications within the computing continuum (edge AI, distributed machine learning, autonomous decision systems), where rapid iteration and deployment are competitively important. Additionally, if regulatory compliance timelines lag technology development cycles, regulations become obsolete before they are fully implemented, creating frustration and encouraging non-compliance. Since innovation is competitive and Europe regulates more strictly than competitors, European innovators face competitive disadvantage, particularly if regulatory burden increases for European companies while non-European competitors operate in less regulated environments. This could create a "brain drain" of AI talent and AI startups from Europe to less regulated jurisdictions.

2. Privacy and Security Concerns Limiting Trust and Adoption
Despite Europe's strong data protection frameworks, practical concerns about privacy and security in cloud and continuum environments remain. Concerns include the difficulty of verifying that cloud providers truly isolate and protect data, uncertainty about insider threats and state-level access requests, lack of transparency about data processing, and complexity of understanding who actually controls data in federated systems. These concerns are not irrational; they reflect real risks that, if not adequately addressed through transparent, verifiable

mechanisms, will constrain adoption of cloud and continuum technologies, particularly in regulated sectors (finance, healthcare, government).

This is a threat because it directly prevents market growth and creates openings for competitors claiming stronger security or data control. Europe has strong regulatory frameworks but lacks practical, verifiable mechanisms for users to confirm that their data is actually protected as promised. Until mechanisms like trusted execution environments, verifiable encryption, transparent audit trails and enforceable data isolation become standard features of cloud and continuum services, adoption will remain limited, reflecting a genuine capability gap that must be addressed to unlock market potential.

3. Energy Costs and Dependence on External Energy Suppliers

Computing continuum technologies are energy-intensive. Data centres, edge computing facilities, and large-scale IoT deployments all require substantial electrical power. If Europe cannot control energy costs and sourcing, continuum deployment becomes uneconomical and creates strategic vulnerability. European energy costs are currently higher than in US and Asia, partly due to energy source diversity (moving away from fossil fuels) and reliance on imported energy.

A threat exists that if Europe does not develop sufficient renewable energy capacity, maintain reasonable energy costs and diversify energy sourcing, computing continuum infrastructure will become economically uncompetitive globally. Additionally, energy dependence creates vulnerability: if external energy suppliers restrict supply for geopolitical reasons, computing continuum operations could be disrupted. Energy costs and dependence directly impact the economics of deploying computing continuum infrastructure. Unlike technology or regulation, which can be improved through policy, energy costs are partly determined by global commodity markets and partly by geography. Europe must proactively manage this threat through renewable energy investment, energy efficiency standards for data centres, and strategic energy sourcing.

4. Lagging Digital Transformation Across Traditional Industries

Europe possesses world-leading traditional industries (automotive, manufacturing, energy, chemicals, pharmaceuticals). However, these industries are digitalising more slowly than required to maintain competitiveness. If these "old economy" sectors do not rapidly adopt cloud, edge, IoT and AI technologies, they risk erosion of competitive position to more digitally advanced competitors. This is particularly critical for Industry 4.0, smart manufacturing, predictive maintenance, supply chain optimisation and digital sustainability tracking all areas where computing continuum technologies are fundamental enablers.

If European traditional industry does not accelerate digital transformation, competitiveness in these sectors will erode, leading to job losses and reduced economic dynamism. This cascades into reduced demand for computing continuum infrastructure in Europe, weakening the business case for European cloud and edge investment. Lagging digital transformation creates a self-reinforcing negative cycle: without strong demand from traditional industries, computing continuum infrastructure investment remains limited; without robust infrastructure, digital transformation becomes difficult. Breaking this cycle requires coordinated action to accelerate traditional industry digital adoption, a task beyond any single company's capacity.

5. Failure to Achieve a True Single Market for Computing Continuum Infrastructure

Despite decades of European integration rhetoric, a genuine single market for telecommunications infrastructure, cloud services and computing continuum technologies does not yet exist. National regulations still fragment the market, spectrum is allocated nationally rather than continentally, and operators must navigate 27 separate regulatory regimes. This fragmentation prevents the scale economies necessary to compete with unified global competitors.

If Europe cannot consolidate toward a true single market, with continent-wide spectrum allocation, reciprocal regulatory recognition, and unified infrastructure governance, computing continuum deployment will remain hobbled by fragmentation. European companies cannot scale to global competitiveness within fragmented national markets; they will continue to be smaller, less efficient and less profitable than consolidated global competitors. This is a fundamentally self-inflicted threat: unlike external competitive threats which require excellence to overcome, market fragmentation is a policy choice. If Europe cannot make the political choices necessary to consolidate markets, it is essentially accepting competitive disadvantage as a permanent condition.

3.2.6 SYNTHESIS

Factor 2 presents a paradoxical strategic situation. Europe possesses world-leading regulatory frameworks that explicitly embed European values (data protection, fair competition, sustainable development, fundamental rights) into digital policy. Instruments such as the AI Act, Data Act, Digital Markets Act, and data sovereignty initiatives (Gaia-X) represent sophisticated, forward-looking governance that is increasingly adopted as global reference standards.

However, these regulatory strengths coexist with significant implementation weaknesses: fragmentation across Member States, excessive and overlapping regulatory requirements, administrative burden that disproportionately harms SMEs, insufficient compliance enforcement, and lack of unified capital markets and infrastructure governance. The result is a situation where Europe has exceptionally strong regulatory intent but inconsistent, fragmented execution. Companies operating in European markets face high compliance costs but inconsistent application; small innovators face bureaucratic barriers that large, well-resourced competitors can absorb; and fragmented national markets prevent the consolidation and scale necessary to compete globally.

Opportunities exist to convert these weaknesses into strengths through strategic reforms: streamlining and consolidating regulations to reduce fragmentation and administrative burden; establishing unified digital governance authorities to ensure consistent implementation; completing the digital single market through harmonisation of telecommunications and infrastructure regulations; significantly expanding strategic investment in semiconductors, quantum computing and computing continuum infrastructure; and scaling successful coordination mechanisms like the IPCEI model. Threats, including overly strict innovation regulation, privacy concerns limiting adoption, energy costs, lagging digital transformation in traditional industries, and persistent market fragmentation, underscore the urgency of moving from regulatory aspiration to implementation excellence.

The central strategic question for Factor 2 is whether Europe can maintain its regulatory leadership and values-based differentiation while simultaneously streamlining implementation, reducing burden and creating the unified market and industrial scale necessary for global competitiveness. This requires political will to make difficult choices: accepting some regulatory harmonisation that creates uniformity rather than perfect Member State customisation; consolidating fragmented infrastructure governance; and making substantial public investments in strategic technologies where private markets alone cannot achieve necessary scale.

3.3 SWOT Factor 3: Enabling Conditions

3.3.1 Context

Factor 3 addresses the cross-cutting prerequisites that facilitate the successful development, implementation and adoption of Cognitive Computing Continuum technologies at scale across the EU. Enabling conditions encompass open-source software and hardware ecosystems, adherence to open and interoperable standards, workforce skills and training capacity, and ethical and societal dimensions such as data protection, cybersecurity, transparency and digital inclusion.

Europe has made strategic commitments to embedding openness, standards alignment and values-based governance into its digital infrastructure. The EU's institutional support for open source, including the European Commission's Open Source Programme Office (established 2020) and initiatives like the European Open Standards Strategy and the Open Standards Platform, demonstrates deliberate positioning. Simultaneously, Europe's legal framework based on GDPR, data protection principles and ethical guidelines creates differentiated governance standards that can attract globally-conscious organisations seeking trustworthy technology environments. However, realising these strengths requires sustained investment in workforce development, corporate engagement with open-source communities and transparent governance of open-source projects.

The central challenge for enabling conditions is to convert Europe's values-based regulatory frameworks and institutional commitments to open standards into operational capabilities: skilled workforces capable of developing and maintaining critical open-source infrastructure; sustained funding mechanisms that support long-term open-source sustainability rather than project-by-project discontinuity; and corporate cultures (particularly in large enterprises) that view open-source participation not as peripheral but as central to technological strategy. Without such operational integration, Europe risks possessing excellent policy frameworks while lacking the human and institutional capacity to execute them.

3.3.2 STRENGTHS

1. The Strength of SMEs in the European Open Source Ecosystem
Small and Medium-sized Enterprises (SMEs) represent a significant and distinctive strength in the European open-source ecosystem. Unlike larger, hierarchical organisations that struggle with open-source governance models, SMEs often operate with flatter structures and collaborative orientations naturally aligned with open-source principles. European SMEs contribute meaningfully to open-source projects, drive innovation through distributed development models, and embody the collaborative ethos that characterises healthy open-source communities.

This SME strength is particularly important for the computing continuum because edge computing and distributed IoT architectures inherently require smaller, specialised solution providers rather than monolithic vendors. SMEs developing open-source edge computing platforms, IoT connectivity solutions and distributed data processing tools are creating the technical foundations of continuum deployment. Their participation ensures that open-source solutions remain responsive to practical needs rather than being driven solely by large vendors' commercial interests. Furthermore, SMEs are geographically distributed across Europe, creating a resilient ecosystem where innovation is not concentrated in a single hub.

2. EC Commitment: Promoting Open Standards and Institutional Leadership

The European Commission has established itself as a deliberate institutional leader in promoting open standards and open-source software. The European Open Standards Strategy, the European Open Standards Platform, and the Digital Single Market initiative all explicitly prioritise open standards in technology adoption. Most significantly, the EC Open Source Programme Office (OSPO), established in 2020, provides organisational infrastructure to facilitate open-source adoption within EU institutions and to coordinate institutional open-source strategy.

Complementary projects, such as Sylva, CAMARA and SIMPL, extend this institutional commitment by creating practical frameworks for open-source integration across different layers of the computing continuum, from hardware to cloud infrastructure and networking. This institutional leadership is consequential because it legitimises open-source as strategic infrastructure rather than a niche or alternative approach. When the EC's own institutions adopt and promote open standards, it signals to private companies and Member States that open-source is a credible, supported trajectory. This institutional backing provides the governance clarity and resource commitment necessary to sustain long-term open-source initiatives.

3. Capacity to Develop European Talent in Open Source

Europe possesses developed educational institutions and training infrastructure capable of systematically developing open-source expertise in new generations of technologists. Universities across Europe offer advanced computer science and software engineering programmes; vocational and technical training systems can be oriented toward open-source technologies; and public sector training programmes can be redesigned to develop open-source competencies. This educational capacity is not yet fully mobilised for open-source skill development, but the institutional infrastructure exists.

The strategic importance of talent development for open source is acute because open-source communities depend fundamentally on human expertise like developers, maintainers, architects and security specialists capable of contributing to and stewarding critical projects. By explicitly integrating open-source education into training systems (from secondary technical education through university and continuing professional education), Europe can ensure that its emerging workforce possesses native competency in open-source development, governance and maintenance. This is particularly important for ensuring that European open-source projects are maintained by European talent rather than becoming dependent on international volunteer communities that may lack long-term commitment.

4. A Strong Framework Based on European Values

The EU has established a comprehensive legal and ethical framework grounded in European values including data protection (GDPR), privacy, cybersecurity, fundamental rights protection and transparent governance. This framework extends into the open-source domain, creating expectations and requirements that open-source projects operated within European contexts must meet high standards for data protection, security and ethical governance.

This values-based framework is a strength because it provides clear guidance for technology development and creates differentiation in global markets. Open-source projects developed and maintained within the European regulatory and values framework can credibly market themselves as "trustworthy" because they operate under binding legal requirements and transparent governance. For organisations in regulated sectors (finance, healthcare, government) that require assurance about ethical governance and legal compliance, European open-source projects offer operational advantages. The framework also attracts globally-conscious developers and organisations who prioritise values alignment over purely technical considerations.

5. Growing Awareness and Momentum for Open Source in Key Member States

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

Several Member States, notably France, Germany and the Netherlands, have adopted explicit national policies promoting open-source adoption in public procurement, digital infrastructure and industrial strategy. France's approach to digital sovereignty explicitly incorporates open-source as a strategic tool; Germany's digital policy increasingly recognises open-source as foundational infrastructure; the Netherlands has been a consistent advocate for open standards. This member-state momentum creates a supportive environment for open-source initiatives and demonstrates political commitment at national and EU levels.

This strength matters operationally because member-state support translates into procurement preferences, regulatory streamlining and funding mechanisms that favour open-source approaches. When national governments commit to open-source-first procurement policies, it creates sustained demand for open-source projects and services, enabling open-source maintainers and service providers to plan long-term investment. Member-state momentum also creates policy alignment that reduces the fragmentation that otherwise hampers European digital initiatives.

6. Good Examples of Open-Source Software in the Public Sector
European public sector organisations, from national administrations to local governments and public services, increasingly leverage open-source software to enhance transparency, foster collaboration, reduce operational costs and drive innovation. Public sector adoption of open-source creates multiple operational advantages: transparency in critical services builds public trust; collaboration between public institutions and open-source communities strengthens both; reduced vendor lock-in and licensing costs free resources for strategic investment; and innovation occurs faster when software source code is visible and modifiable by multiple institutions.

These public sector examples are strength because they demonstrate viability and create reference implementations for other public and private organisations. When a government service delivers core functions using open-source software, it proves that open-source is suitable for critical, regulated, high-availability systems. Additionally, public sector participation in open-source projects, by publishing code, engaging with communities and employing open-source developers, strengthens the broader European open-source ecosystem by bringing institutional resources and long-term commitment.

3.3.3 WEAKNESSES

1. Shortage of Skills and Lack of Open-Source Development Capacity
Despite SME strengths, Europe faces a structural shortage of teams with advanced capabilities in developing, maintaining and evolving open-source software and hardware. This is a continental problem, not unique to Europe, but it affects Europe particularly acutely given fragmentation across 27 Member States and variable technical capacity across regions. The shortage manifests as difficulty attracting software developers with open-source specialisation, limited capacity to maintain critical open-source projects over multi-year horizons and insufficient expertise in open-source security and governance.

This skills shortage is particularly damaging for critical infrastructure projects where open-source maintenance cannot be intermittent or volunteer-dependent. A vulnerability discovered in a critical open-source component requires rapid response from experienced maintainers; if Europe lacks such expertise, critical infrastructure becomes vulnerable. The shortage also creates a vicious cycle: without strong employment opportunities in open-source development, talented developers are drawn to proprietary software companies; without sufficient developers, open-source projects cannot commit to rapid iteration and advanced feature development; without advanced capabilities, projects remain less competitive than proprietary alternatives, further reducing developer interest.

Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

2. Lack of Open-Source Governance and Limited Corporate Engagement
European companies, particularly large enterprises, tend to engage less actively with open-source projects than their US and Chinese counterparts. While US companies routinely employ engineers dedicated to maintaining core open-source projects, European companies often treat open-source as incidental, using open-source code but contributing minimally to governance and development. This creates a governance asymmetry: European companies benefit from open-source infrastructure but do not invest proportionally in its stewardship.

The lack of corporate engagement is particularly concerning for open-source governance in edge-cloud-IoT domains, where architectural decisions made early in project governance can shape development trajectories for years. If European companies do not participate actively in governance, their interests and values may not shape project direction. Additionally, the EU's open-source landscape remains fragmented, with multiple overlapping initiatives (as noted in other factors) but insufficient coordination or governance alignment. This fragmentation reduces the effectiveness of individual projects and prevents the ecosystem-level coherence necessary for the computing continuum.

3. Lack of Funding for Open-Source Development and Maintenance
Open-source projects struggle to attract venture capital and sustained private investment compared to proprietary software ventures, partly because open-source business models are less straightforward and investor returns are less transparent. While public programmes like Horizon Europe provide substantial funding, it is typically project-based with limited sustainability beyond the funding period. Once project funding ends, maintainers must transition to commercial models (offering services, consulting, commercial distributions) or face funding discontinuity.

This lack of sustained funding is a weakness because it creates brittleness in critical infrastructure. A maintenance gap between the end of one funding cycle and the beginning of the next can result in security vulnerabilities remaining unpatched, feature requests accumulating and developer burnout. For the computing continuum, which depends fundamentally on open-source software across multiple layers (operating systems, networking, data processing, edge computing platforms), funding discontinuity creates systemic vulnerability. More targeted funding mechanisms specifically designed for long-term open-source sustainability, rather than project-based grants, are essential.

4. Lack of Corporate Understanding of Open Source's Strategic Importance
Within the EU, recognition of open-source's strategic importance is growing but remains less deeply embedded in corporate culture than in the US or China. Many large European companies still view open-source as a cost-cutting measure (using free software) rather than as a strategic capability (investing in open-source development and governance). This cultural gap means that investment in open-source capabilities, employment of open-source developers and participation in open-source governance remain underemphasised in corporate strategy.

This cultural weakness has cascading effects. Without strong corporate support, open-source initiatives struggle to attract necessary resources, talent and investment. Talented developers may pursue employment in proprietary software companies where investment and career advancement are more visible. Open-source projects may struggle to access infrastructure, testing facilities and quality assurance resources that corporate backing could provide. For the computing continuum, which requires integration across multiple open-source components, lack of corporate support means that individual projects remain isolated rather than being coordinated into coherent ecosystems.

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

3.3.4 OPPORTUNITIES

1. Programmes Fostering Open-Source Development and Digital Competencies

Initiatives like StandICT and NGI Commons programmes have demonstrated viability in funding open-source development and building digital competencies. An opportunity exists to significantly expand these programmes, making them more systematic and longer-term. This expansion should include explicit funding for open-source project governance, security auditing, and long-term maintenance, areas currently underfunded. Additionally, these programmes should be explicitly connected to skills development and workforce training, creating pathways from educational programmes into sustained open-source employment.

Expanding these programmes creates competitive advantage because it builds a durable, EU-level open-source ecosystem that is less dependent on individual volunteer efforts or single companies' commitments. When public funding systematically supports open-source development and attracts talented developers to this sector, Europe develops distinctive capabilities in open-source stewardship that are difficult for competitors to replicate. This is particularly important for the computing continuum, where sustainable, well-maintained open-source foundations are essential.

2. Promoting Open Hardware Initiatives for Technological Sovereignty

Open hardware represents a frontier domain where Europe can achieve distinctive advantage. The EU has recognised open hardware's importance and has begun supporting its development, with contributions from both public research institutions and private companies. Open hardware offers multiple benefits: technological sovereignty (reducing dependence on proprietary hardware designs), innovation (enabling rapid customisation and experimentation), cost savings (avoiding proprietary licensing and manufacturing lock-in) and customisation (enabling hardware tailored to specific continuum applications).

Promoting open hardware is an opportunity because it extends the principles of openness and interoperability from software into the physical layer of the computing continuum. For edge computing devices, IoT sensors and interconnection hardware, open-source designs enable European companies and public institutions to avoid dependence on non-European hardware vendors. Additionally, open hardware development creates employment opportunities for hardware engineers, manufacturing specialists and designers, labour categories important for European industrial competitiveness.

3. Attracting Open-Source Talent to Europe

Europe can differentiate itself as an attractive destination for open-source talent globally by emphasising its values-based governance framework, strong legal protections (particularly for employee rights, data protection and privacy), and commitment to open-source as strategic infrastructure. Countries and regions that offer less political stability, weaker legal protections or less explicit commitment to openness may lose talent to Europe. European institutions can deliberately position open-source careers, research positions, engineering roles, governance leadership, as opportunities to work on infrastructure that reflects European values and serves a values-aligned user base.

This represents an opportunity to overcome talent shortage not only through training Europeans but by attracting globally-talented open-source developers to European institutions. When globally-recognised open-source developers choose to base their work in Europe, it strengthens the entire ecosystem by bringing expertise, reputation and international collaborative networks. This is particularly important for projects serving regulated sectors (finance, healthcare, government) where trust in developer identity and jurisdiction is important.

Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

4. Open Source Solutions for Addressing Ethical and Social Challenges
Open-source approaches are inherently suited to addressing ethical and social challenges in edge-cloud-IoT systems because transparency, auditability and community governance are built into open-source models. A malicious actor attempting to embed data harvesting, privacy violations or unethical decision logic into open-source code faces immediate detection by the community. This transparency is particularly important for AI systems and automated decision systems where ethical concerns are acute.

This represents an opportunity to position open-source not merely as a technical alternative but as an ethical framework for technology development. Organisations concerned about data privacy, algorithmic transparency, vendor lock-in and ethical governance have strong reasons to prefer open-source solutions. For the computing continuum, which will increasingly incorporate AI and automated decision-making at edge, cloud and IoT layers, open-source approaches offer operational assurance that closed proprietary systems cannot provide. Explicitly promoting open-source as an ethical framework can attract organisations (particularly public sector institutions) to open-source adoption.

5. Open-Source Software as Sustainability Enabler
Open-source software offers significant potential for sustainability, reducing energy consumption through efficient code, avoiding redundant proprietary implementations that consume computational resources, and enabling communities to collectively optimise for sustainability rather than vendors optimising for proprietary feature differentiation. Additionally, open-source software avoids vendor lock-in and vendor-driven obsolescence, reducing the need for frequent technology replacement and the associated environmental impact.

This represents an opportunity to explicitly integrate open-source into Europe's Green Deal and sustainability objectives. Open-source software development should be seen as integral to achieving climate and sustainability goals, not peripheral to them. By promoting open-source as a sustainability tool and funding open-source projects explicitly for sustainability optimisation, Europe can align technological development with environmental objectives while building distinctive capability in sustainable software development, an increasingly important market differentiator.

3.3.5 THREATS

1. Lack of Resources for Maintenance and Scalability
As Europe invests in expanding open-source initiatives, the maintenance burden on core projects increases. Without sustained investment in technical skills, infrastructure and governance capacity, individual open-source projects may be overwhelmed by adoption demands. A project designed for research use may suddenly face production demands from industry; without sufficient maintainer capacity, quality and security decline. Additionally, as continuum deployment increases, the criticality of open-source infrastructure increases: a failure in a widely-deployed edge operating system affects far more systems than it did when adoption was limited.

This threat is self-inflicted through success: the more Europe invests in open-source adoption, the greater the maintenance burden becomes. Without deliberate planning for maintenance scalability, including sustained funding, additional maintainer recruitment and infrastructure investment, rapid expansion of open-source adoption could create a brittleness where popular projects lack sufficient resources to handle demand, leading to security vulnerabilities and feature stagnation.

2. Misunderstanding and Dismissal of Open-Source by Large Technology Companies
Despite growing recognition, large technology companies sometimes treat open-source with skepticism or misunderstanding, viewing it as a threat to proprietary business models rather

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

than as a tool for strategic positioning. Some companies actively lobby against open-source policy initiatives, argue that open-source creates liability risks and attempt to persuade policymakers that proprietary approaches are more secure or reliable. This lobbying narrative, though often factually incorrect, can influence policymakers unfamiliar with open-source realities.

This threat is concerning because it can undermine the policy and regulatory environment supporting open-source. If large companies successfully convince governments that open-source represents regulatory or security risks, policies may shift against open-source adoption in critical sectors. Additionally, some large companies may position themselves as the only "safe" alternative to risky open-source, effectively consolidating market control. Countering this threat requires clear communication about open-source benefits and ongoing policy education of decision-makers.

3.3.6 SYNTHESIS

Factor 3 characterises a landscape where Europe possesses strong institutional commitments to open-source and open standards, growing member-state political support, and distinctive SME ecosystem participation in open-source communities. Regulatory frameworks based on European values create operational advantages for trustworthy open-source development. However, these strengths coexist with significant structural weaknesses: shortage of skilled open-source developers, limited corporate engagement in open-source governance despite reliance on open-source code, insufficient sustained funding mechanisms and cultural gaps where open-source is not yet deeply embedded in corporate strategy.

Concrete opportunities exist to convert these weaknesses into strengths through systematic expansion of open-source funding programmes, promotion of open hardware as sovereignty tool, deliberate talent attraction globally, explicit integration of open-source into sustainability objectives and positioning of open-source as ethical governance framework. Threats, including maintenance and scalability risks as adoption expands and large company lobbying against open-source, underscore the need for sustained, coordinated investment in open-source as essential infrastructure.

The central strategic question for Factor 3 is whether Europe can transition from rhetorical commitment to open-source toward operational integration where open-source development and maintenance are treated as critical infrastructure requiring the same sustained investment and talent development as any other foundational technology. This requires overcoming corporate cultural barriers, establishing sustained funding mechanisms independent of project cycles, and developing open-source governance expertise within both public institutions and private companies.

3.4 SWOT Factor 4: Infrastructures and Connectivity

3.4.1 Context

Factor 4 encompasses the physical and logical infrastructure layers that enable the Cognitive Computing Continuum: data centre networks, 5G/6G connectivity, terrestrial and space-based infrastructure, data platforms and backbone networks. This factor addresses the "where" and "how" of computing continuum deployment, the material substrate and connectivity fabric that determine whether continuum architectures can function at scale and across borders.

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

Europe possesses a diverse and technologically advanced infrastructure base, including federated data centre initiatives (Gaia-X, Structura-X, SIMPL, Sovereign-X, INFRA-X) designed to ensure digital sovereignty while maintaining interoperability. Major telecommunications suppliers (Ericsson, Nokia) provide competitive alternative to non-European vendors in critical 5G and edge computing infrastructure. Simultaneously, Europe faces critical infrastructure gaps: insufficient renewable energy capacity to support energy-intensive data centre and AI infrastructure economically; fragmented investment in 5G/6G and fibre optics across Member States; reliance of SMEs on non-European hyperscalers (AWS, Azure, Google Cloud) due to gaps in European alternatives; and high energy costs that make European infrastructure less economically competitive globally than infrastructure in US and Asia.

The central challenge for infrastructures and connectivity is to close these gaps while maintaining Europe's values-based governance and data sovereignty objectives. This requires simultaneous advances across multiple fronts: accelerating deployment of renewable energy and achieving energy efficiency in data centres; achieving unified European telecommunications standards and spectrum allocation; completing fibre and 5G infrastructure deployment across all regions; developing competitive European cloud and edge infrastructure alternatives that can serve SMEs without requiring hyperscaler dependence; and integrating space-based infrastructure (satellites, space connectivity) into the terrestrial continuum architecture.

3.4.2 STRENGTHS

1. Diverse and Advanced Technological Infrastructure with Federated Architecture
Europe has accumulated over decades a sophisticated and geographically distributed computing infrastructure comprising edge nodes, specialised data centres and high-capacity interconnection networks. This diversity reflects sustained public and private investment in infrastructure and increasingly reflects strategic orientation toward distributed and federated architectures suited to edge-cloud-IoT continuum deployment.

Initiatives such as Gaia-X play a central coordinating role, designed as a federated framework to guarantee digital sovereignty through interoperability among heterogeneous edge, cloud and IoT service providers, allowing data and services to be shared under clear European rules. Complementary projects, Structura-X (creating federated cloud infrastructure aligned with Gaia-X standards), SIMPL (facilitating interoperability and secure data access), Sovereign-X and INFRA-X, consolidate an architecture capable of supporting complex computing continuum applications across sectors and borders. The Important Project of Common European Interest on Next-Generation Cloud Infrastructure and Services (IPCEI-CIS) marks a significant commitment to developing alternatives to hyperscaler-dominated platforms, with additional IPCEIs planned for Artificial Intelligence and Cloud Infrastructures. This combination of federated governance frameworks and large-scale coordinated investment creates a distinctive European approach to infrastructure, one oriented toward interoperability, decentralisation and values-based sovereignty rather than vendor lock-in.

2. Robust European Telecommunications Equipment Suppliers
Europe hosts globally leading telecommunications equipment suppliers, notably Ericsson and Nokia, whose market presence, technological credibility and continuous innovation in 5G, 6G and edge computing represent a strategic infrastructure asset. These companies are frontier technology developers, not merely hardware vendors, with leadership in radio access networks, edge processing, network virtualisation and distributed orchestration. Their technological strength ensures that Europe has credible domestic alternatives to non-European vendors, reducing strategic dependency for critical telecommunications infrastructure.

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

This telecommunications supplier strength is particularly significant in contexts of rising geopolitical tensions, where the availability of trusted suppliers becomes a national and European security factor. The presence of robust European vendors reduces dependence on non-European actors for critical network infrastructure and enables Member States and operators to base long-term cooperation on shared values, regulatory alignment and predictable governance. Additionally, these companies drive innovation in areas critical to the computing continuum, edge processing capabilities, distributed resource orchestration and network virtualization, ensuring that European infrastructure evolves with cutting-edge technologies rather than remaining dependent on non-European vendors' product roadmaps.

3. Cyber Resilience Act and NIS2 as Infrastructure Security Framework
The Cyber Resilience Act (CRA) and Network and Information Security Directive 2 (NIS2) establish a unified cybersecurity framework for EU digital infrastructure and services. Rather than fragmented national cybersecurity requirements, these regulations create coherent standards that protect infrastructure integrity while establishing clear compliance pathways. For SMEs, while implementation requires initial investment, compliance provides competitive advantages: protection against data breaches, reduced financial losses from security incidents and ability to market compliance as trust signal to customers and partners.

These regulatory frameworks strengthen infrastructure by creating systematic security standards rather than ad-hoc security practices. Over time, CRA and NIS2 compliance creates an infrastructure ecosystem where security is built-in rather than bolted-on, reducing vulnerability to emerging threats. For the computing continuum, where security risks propagate across interconnected edge, cloud and IoT nodes, unified security standards are essential. Organisations operating under consistent security frameworks can collaboratively share threat intelligence and coordinate security responses more effectively than organisations operating under fragmented national requirements.

4. Data Ownership and Data Spaces as Governance Frameworks
Europe's emphasis on data ownership, ensuring that individuals and organisations control their own data, combined with development of data spaces (common standards and frameworks for data sharing across organisations and sectors) creates a distinctive governance approach to distributed data. Data spaces facilitate interoperability by providing common standards while enabling organisations to maintain data control. Data sovereignty frameworks ensure that data remains within EU jurisdiction, enhancing strategic autonomy and reducing dependence on non-European platforms for data management.

This governance approach is important for continuum infrastructure because continuum deployment necessarily involves data flowing across multiple nodes, from edge devices to cloud processing centres to storage systems. Without clear data ownership and space governance frameworks, continuum infrastructure could inadvertently create data concentration and lock-in. By explicitly embedding data ownership and space governance into infrastructure design, Europe creates infrastructure that serves users' interests rather than vendor interests. This is particularly important for regulated sectors (finance, healthcare, government) where data control is non-negotiable.

3.4.3 WEAKNESSES

1. SME Dependence on Non-European Hyperscalers for Digital Infrastructure
SMEs across Europe rely on global hyperscalers (AWS, Microsoft Azure, Google Cloud) for digital infrastructure because these providers offer extensive, scalable, reliable services with global reach. This reliance undermines EU digital sovereignty objectives by increasing dependency on non-European technologies and services. SMEs face significant barriers to adopting European alternatives: European solutions are often fragmented across providers and lack the integrated service ecosystem of hyperscalers; regulatory complexity in navigating

EU requirements discourages SMEs from taking on integration complexity; and cost advantages of hyperscalers (driven by global scale economies) make European alternatives appear expensive.

This dependence creates operational vulnerability: if hyperscalers restrict service access for geopolitical or commercial reasons, SMEs lack alternatives. It also creates data vulnerability: SME data is stored and processed on non-European infrastructure, subject to non-European legal jurisdictions and potentially accessible to non-European governments. For SMEs in regulated sectors, this creates compliance friction: how can they ensure GDPR compliance if data is physically located on non-European servers? The weakness is structural: until European infrastructure alternatives achieve comparable scale, service integration and cost competitiveness, SME hyperscaler dependence will persist.

2. Insufficient European Infrastructure and Lack of Unified Approach

Europe's current computing infrastructure is insufficient to support future computing needs, particularly given the energy demands of generative AI and the growing data volumes flowing through continuum systems. Europe has effectively conceded the hyperscaler market to non-European players, recognising that building continent-scale cloud providers comparable to AWS, Azure or Google Cloud would require investments of such magnitude that individual European companies and even Member States cannot justify them. This creates a paradox: Europe needs large-scale cloud infrastructure to reduce hyperscaler dependence, but individual European actors cannot economically build such infrastructure.

This infrastructure gap is reflected in fragmented data centre markets across Member States, absence of unified spectrum allocation strategies, inconsistent 5G deployment timelines and limited investment in fibre-optic backbone infrastructure. Without unified approach and continent-level coordination, European infrastructure remains a collection of fragmented national systems rather than a coherent European platform. This fragmentation directly undermines competitiveness: European companies cannot scale infrastructure investments across borders, infrastructure costs remain higher than in unified US or China markets, and innovation in distributed infrastructure is slowed by lack of standards coordination. The result is that Europe risks remaining a user of non-European infrastructure rather than a creator and controller of its own technological substrate.

3. Europe's High Energy Costs and Insufficient Renewable Capacity

Computing continuum technologies (particularly data centres, AI computing facilities and large-scale IoT deployments) are energy-intensive. European energy costs are currently two to three times higher than in Asia or the US, partly due to Europe's commitment to renewable energy transition and reliance on imported energy. Additionally, Europe's energy generation capacity is insufficient to support the explosive growth in computing infrastructure demand driven by AI, big data and continuum deployment.

This energy weakness creates economic uncompetitiveness: data centre operators choosing between European and US locations face significantly higher operating costs in Europe, making European infrastructure economically unattractive. It also creates strategic vulnerability: if Europe cannot generate sufficient renewable energy domestically, it remains dependent on energy imports, creating exposure to external supply disruptions. Energy scarcity can also constrain economic growth: energy-intensive industries and technologies are deterred from locating in Europe, slowing innovation and development. For the computing continuum specifically, energy costs directly impact the viability of distributed edge infrastructure: edge nodes must be powered locally, and if local energy costs are prohibitively high, edge deployment becomes economically unviable.

4. Fragmented Digital Infrastructure and Inconsistent 5G/6G and Fibre Investment

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

Europe's digital infrastructure remains fragmented across Member States with inconsistent investment in 5G/6G deployment, fibre optic backbone networks and edge computing facilities. The data centre market is fragmented rather than unified; investment in high-speed connectivity varies significantly by geography; and decentralised network architectures (essential for computing continuum) are unevenly deployed. This fragmentation has multiple negative consequences: infrastructure operators cannot achieve the scale economies of unified markets; companies cannot deploy services on consistent technical foundations across Europe; and interoperability challenges proliferate as different regions use incompatible infrastructure standards.

This fragmentation directly prevents efficient continuum deployment. The computing continuum fundamentally requires consistent, interconnected infrastructure across borders and regions. When 5G availability, fibre connectivity and edge computing infrastructure vary significantly by location, applications cannot depend on consistent service quality and must be designed for lowest-common-denominator conditions. This severely limits the advanced continuum capabilities (real-time processing, low-latency edge computing, distributed AI) that justify continuum investment. Additionally, fragmentation increases infrastructure costs: operators must maintain multiple incompatible systems rather than standardising on single platforms that can achieve efficiency through scale.

3.4.4 OPPORTUNITIES

1. Enhancing EU Computing and AI Infrastructure Through Coordinated Investment
A strategic opportunity exists to rapidly enhance Europe's computing infrastructure and AI capabilities through coordinated public investment in high-performance computing, development of open computing infrastructures that transition from research to commercial availability, and interconnection of public and private computing nodes into unified European ecosystems. The Euro-HPC (European High Performance Computing) initiative provides the institutional framework; expansion of this programme could fund additional facilities, upgrade existing ones and create business models where research computing capacity is made available to SMEs and startups.

This coordinated investment approach addresses the fundamental challenge that no individual European company can economically build hyperscaler-scale infrastructure. However, public investment in shared infrastructure, similar to how universities operate shared research facilities, can provide capabilities that SMEs can access through service models, effectively giving SMEs access to computing capacity without requiring them to build their own infrastructure or depend on non-European hyperscalers. Additionally, public computing infrastructure can be explicitly designed for European compliance with data sovereignty, GDPR and other regulatory frameworks, solving the regulatory friction that SMEs face when adopting non-European cloud services.

2. Streamlining Network Deployment by Consolidating Regulatory Frameworks
A significant opportunity exists to accelerate 5G/6G and fibre-optic deployment by consolidating the Gigabit Infrastructure Act and removing administrative burdens that hamper network deployment. Network deployment faces bureaucratic obstacles at multiple levels: environmental approvals, spectrum allocation procedures, site acquisition, infrastructure sharing negotiations. Consolidating these procedures into unified processes and establishing clear timelines would dramatically accelerate deployment.

This opportunity directly addresses infrastructure fragmentation by reducing the time and cost of network deployment across Member States. When deployment becomes faster and cheaper, operators are incentivized to deploy across larger geographic areas rather than limiting deployment to high-density profitable regions. This drives infrastructure coverage toward less-profitable areas and accelerates the transition toward continent-wide infrastructure

Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

unity. For 5G and fibre deployment specifically, streamlining can reduce deployment timelines from years to months in some contexts, enabling Europe to catch up with global deployment timelines and reduce infrastructure gaps relative to competitors.

3. Creating Common European Cloud-Edge Infrastructure Based on Open Principles

A strategic opportunity exists to develop a coherent common cloud-edge infrastructure for Europe based on principles of openness, interoperability, security, sustainability and vendor neutrality. Rather than fragmenting across competing proprietary platforms, this infrastructure would be explicitly designed for interoperability, allowing SMEs to avoid vendor lock-in while ensuring that European values and governance principles are embedded into infrastructure operations.

This opportunity directly addresses multiple weaknesses: the SME hyperscaler dependence problem (by providing competitive European alternative); the infrastructure fragmentation problem (by establishing common standards and reference architectures); and the data sovereignty problem (by ensuring infrastructure is operated under European jurisdiction with explicit data protection governance). Designing this infrastructure based on open principles also ensures that innovation is not captured by single vendors and that the infrastructure can be continuously improved through distributed innovation rather than depending on vendor product roadmaps.

4. Integrating AI Factories with High-Performance Computing

The integration of AI Factories (large-scale AI processing and training facilities) with Europe's HPC infrastructure represents a strategic opportunity to position Europe as an AI innovation leader while ensuring technological independence. By connecting HPC capacity with AI-specific processing (GPUs, TPUs, quantum computing) and creating business models where researchers and companies can access integrated AI computing capacity, Europe creates distinctive capability for AI model development and deployment.

This opportunity is important because AI capabilities are increasingly central to the computing continuum, particularly for edge intelligence and distributed ML applications. By ensuring Europe develops its own integrated AI computing infrastructure rather than depending on non-European AI service providers, Europe protects strategic autonomy in an increasingly AI-driven economy. Additionally, integrating AI capacity with research institutions enables knowledge transfer from fundamental AI research into practical commercial applications, accelerating the timeline from research breakthrough to market deployment.

5. Connecting European Infrastructure Initiatives to Testing and Experimentation Facilities

A significant opportunity exists to systematically connect European infrastructure initiatives (data centres, edge computing facilities, 5G networks) to Testing and Experimentation Facilities (TEFs) and other open innovation spaces. TEFs provide environments where companies, researchers and startups can test new technologies on real infrastructure before full commercial deployment. By explicitly integrating TEFs with computing continuum infrastructure, Europe creates pathways for startups and SMEs to experiment with continuum technologies without requiring massive capital investment in proprietary test environments.

This opportunity accelerates continuum innovation by reducing barriers to experimentation. When TEFs are accessible and free or low-cost for qualifying users, startups can validate business models and technical approaches before committing to commercial infrastructure. This drives innovation in continuum technologies and creates a pipeline of validated solutions that can transition into commercial deployment. For SMEs particularly, TEF access to real infrastructure is often the difference between pursuing continuum opportunities or remaining confined to traditional computing models.

Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

3.4.5 THREATS

1. Security Vulnerabilities in Complex Distributed Infrastructure
The growing complexity of continuum infrastructure, combining edge devices, local processing, cloud centres, data spaces and interconnection networks, creates expanding attack surface for cybersecurity threats. The increasing adoption of open-source software in critical infrastructures, while providing transparency benefits, also creates security risks if open-source projects lack sufficient resources for security maintenance and vulnerability patching. Malicious actors can exploit vulnerabilities in any node of the continuum to compromise entire systems; supply chain attacks can compromise software or hardware before deployment; and insider threats can undermine infrastructure security despite external defences.

This threat is particularly acute because continuum architectures make security management more difficult than traditional centralised systems. In a centralised data centre, security can be tightly controlled from a single point. In a distributed continuum, security depends on coordinated practices across hundreds or thousands of independent nodes operated by different organisations. Ensuring consistent security practices across this diversity is inherently challenging. Additionally, the speed of continuum deployment, driven by regulatory timelines and market competition, can outpace security hardening, creating windows of vulnerability before comprehensive security practices are established.

2. Global Geopolitics and US Policy Uncertainty
Geopolitical tensions between the EU and non-European powers, particularly uncertainty regarding US administration policies toward European digital autonomy, create threats to European infrastructure development. Recent political shifts create uncertainty about whether the US will support, tolerate or actively oppose European infrastructure initiatives aimed at reducing dependence on US technology providers. Trade restrictions, technology export controls or sanctions could disrupt European access to critical hardware, software or components necessary for infrastructure deployment.

This threat is beyond Europe's direct control but creates uncertainty that inhibits long-term infrastructure investment. Companies and governments hesitate to make multi-year infrastructure commitments when geopolitical conditions could fundamentally change mid-project. Additionally, if US policy turns toward restricting European technology development (for example, through export controls on advanced semiconductors or AI software), European infrastructure initiatives could face sudden constraints. While European infrastructure development aims to reduce dependence, it cannot eliminate it entirely, particularly in cutting-edge domains where global supply chains remain necessary.

3.4.6 SYNTHESIS

Factor 4 presents a landscape where Europe possesses technologically advanced infrastructure components (federated data centres, telecommunications suppliers, cybersecurity frameworks, data governance models) but lacks the unified, large-scale infrastructure that would make the computing continuum economically viable and operationally cohesive across the continent. Europe's commitment to digital sovereignty and values-based governance creates distinctive infrastructure principles, but these principles cannot be realised without addressing critical resource gaps: insufficient renewable energy capacity to support energy-intensive infrastructure; fragmented investment in 5G/6G and fibre deployment across Member States; and structural disadvantage in competing with unified, large-scale infrastructure markets in the US and Asia.

Opportunities exist to address these gaps through coordinated public investment in shared computing infrastructure, streamlining of network deployment regulations, development of common cloud-edge infrastructure based on open principles, and integration of AI capabilities

Funded by the European Union

Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

with HPC. These investments would convert infrastructure fragmentation (weakness) into continental unity (strength) while maintaining European values-based governance. Threats, including expanding security vulnerabilities in complex systems and geopolitical uncertainty regarding US policies, underscore the urgency of achieving infrastructure consolidation and autonomy.

The central strategic question for Factor 4 is whether Europe can mobilise sufficient public investment and political coordination to build unified, continent-scale infrastructure that can serve as credible alternative to non-European hyperscalers, while maintaining the renewable energy investments necessary for long-term sustainability and competitiveness. This requires moving beyond project-based initiatives toward systemic infrastructure strategy with multi-decade timescales and multi-billion euro commitments.

3.5 SWOT Factor 5: Collaboration and Engagement

3.5.1 Context

Factor 5 examines mechanisms for coordination and alignment among European initiatives, between European and international actors, and across public-private partnerships. This factor addresses fragmentation and seeks to ensure that the computing continuum becomes a genuinely European endeavour rather than a collection of disconnected national, institutional or sectoral projects. Collaboration and engagement determine whether Europe's technological, regulatory and infrastructural components are orchestrated into coherent strategy or remain isolated efforts.

Europe has established multisectoral collaboration initiatives (Sylva, CAMARA, ApeiroRA) that bring together leading European telecommunications, technology and manufacturing companies. The IPCEI-CIS initiative, with €2.6 billion in combined public and private investment and over 100 industrial partners from 12 Member States, demonstrates continent-scale coordination capacity. Additionally, Europe has begun developing strategic partnerships with aligned international actors, particularly Japan, where alignment on data protection, digital sovereignty and values-based governance creates potential for collaborative innovation. However, significant weaknesses persist: fragmentation among overlapping EU initiatives that duplicate efforts rather than coordinate; ineffectiveness of Digital Innovation Hubs in supporting SMEs and startups; limited participation from SMEs in large initiatives; and dependence on established US cloud contracts that lock-in public sector buyers and limit room for European alternatives.

The central challenge for collaboration is to convert Europe's numerous initiatives into coherent ecosystem where participants understand their roles, avoid duplication and coordinate toward shared objectives. This requires governance mechanisms that ensure transparency, accountability and alignment; it requires explicitly including SMEs and startups in governance, not merely as beneficiaries of projects designed by large companies; and it requires strategic partnerships with aligned international actors that create genuine reciprocity rather than one-way dependence.

Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

3.5.2 STRENGTHS

1. Multisectoral Collaboration Initiatives Demonstrating Coordination Capacity
Europe has developed multisectoral collaboration initiatives (Sylva, CAMARA and ApeiroRA) that bring together leading European telecommunications, technology and manufacturing companies around shared objectives for digital sovereignty and secure infrastructure. These initiatives facilitate knowledge exchange, align technical strategies and establish governance models where companies with historically competitive relationships can collaborate on shared problems. The existence of these platforms demonstrates that European companies possess capacity and willingness to collaborate on strategic challenges, overcoming competitive silos that might otherwise prevent coordinated action.

These collaboration initiatives are strengths because they establish working relationships and governance mechanisms that can scale beyond individual projects. When telecommunications companies collaborate on interoperability standards through CAMARA, they create technical foundations that SMEs and startups can build upon without duplicating standards development work. When companies collaborate through Sylva on open connectivity standards, they establish trust relationships and governance practices that can be extended to other domains. For the computing continuum, these multisectoral initiatives are crucial because the continuum inherently requires coordination across telecommunications, cloud, edge, IoT and application-layer companies, domains that have historically operated independently.

2. IPCEI-CIS as Large-Scale Coordinated Investment Model
The Important Project of Common European Interest on Cloud Infrastructure and Services (IPCEI-CIS) represents an unprecedented scale of coordinated European investment: €2.6 billion in combined public (€1.2 billion) and private (€1.4 billion) investment across over 100 industrial partners from 12 Member States. This scale of coordination demonstrates that European actors can overcome fragmentation and align around shared objectives when institutional mechanisms (IPCEI structure) and political commitment (Member State support) enable it.

IPCEI-CIS is particularly significant because it explicitly aims at creating alternatives to non-European cloud providers while maintaining interoperability standards that prevent vendor lock-in. By pooling resources at IPCEI scale, European companies achieve investment levels that no individual company or Member State could justify independently. The initiative creates common infrastructure, shared standards and collaborative governance that benefit the entire European ecosystem. Additionally, IPCEI-CIS demonstrates viability of the IPCEI model for computing continuum: the success of IPCEI-CIS has already prompted planning for additional IPCEIs in AI and cloud infrastructure, extending the model to adjacent domains.

3. Federated Service Model Demonstrated by International Partners
Japan's approach to providing telecommunications and infrastructure services demonstrates viability of federated service models where multiple independent providers operate under common standards and governance frameworks to compete while maintaining interoperability. This model proves that "natural monopoly" arguments used to justify consolidation can be overcome through federated governance that enables competition while preventing fragmentation.

This international example is relevant to the computing continuum because Europe is pursuing similar federated approaches (Gaia-X) but lacks operational precedents at large scale. Japanese experience provides proof of concept that federated models can function in practice, maintain service quality and foster innovation despite apparent advantages of unified provision. By studying Japanese federated infrastructure approaches, European policymakers and companies can accelerate learning about governance mechanisms, competitive dynamics and risk mitigation strategies appropriate for federated continuum infrastructure.

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

4. Aligned International Partnership with Japan on Digital Governance

Japan's alignment with European digital policy, particularly on data protection, digital sovereignty and values-based governance, creates opportunity for genuine strategic partnership. Japan's influential industrial association (Keidanren) often aligns more closely with EU digital policy than with US policy; Japan has adopted data protection frameworks similar to GDPR; and Japan faces similar strategic autonomy challenges relative to US technology dominance. This alignment suggests potential for deep partnership on continuum governance rather than superficial collaboration.

The EU-Japan Digital Partnership provides institutional framework for this collaboration. Additionally, Japan's strengths in automotive and industrial sectors align with European strengths, creating potential for joint solutions addressing Industry 4.0, edge intelligence and distributed manufacturing. Most importantly, Japan's independence from US technology ecosystems and commitment to alternative technology pathways creates possibilities for joint development of continuum technologies that neither Europe nor Japan could develop independently but together could create. This is particularly significant for areas like open hardware, federated governance models and values-based AI development.

5. Japanese Government and Industry Openness to Interoperability

Recent developments in Japan, including the IT Promotion Agency's (IPA) development of Edge/IoT strategy and Fujitsu's success in securing major government cloud contracts in competition with US providers, demonstrate Japanese government openness to supporting local alternatives to dominant US providers. This openness creates opportunity for EU-Japan collaboration where both regions pursue alternatives to US technology dominance through mutually beneficial technological partnerships.

This openness is significant because it indicates that Japan is not content with accepting US technology dominance and is actively seeking alternatives. When combined with European commitment to digital sovereignty, this creates potential for genuine "coopetition" where European and Japanese actors collaborate on continuum technologies that serve both regions' interests in maintaining technological alternatives to dominant global providers. Such collaboration could address specific domains (edge computing, IoT connectivity, AI processing) where neither region has achieved parity with US dominance but together could establish credible alternatives.

6. EU-Japan Digital Partnership as Strategic Foundation

The EU-Japan Digital Partnership provides institutional foundation for advocating pooled digital sovereignty and market interoperability. This partnership has established working relationships, shared objectives on data protection and digital governance, and mechanisms for discussing technology policy. Building on this foundation, the partnership can become vehicle for advancing computing continuum collaboration that serves both regions' interests in achieving technological autonomy while maintaining alignment on values-based governance.

This partnership is a strength because it provides existing institutional mechanism to formalise continuum collaboration without requiring entirely new governance structures. By explicitly expanding the partnership to address computing continuum development, Europe and Japan can coordinate investments, align technical standards and create market opportunities for both regions' companies. For SMEs and startups, EU-Japan partnership coordination creates larger addressable markets and access to complementary technologies without requiring them to navigate complex international partnerships independently.

3.5.3 WEAKNESSES

1. Ineffectiveness of Digital Innovation Hubs in Supporting SMEs and Startups
Digital Innovation Hubs (DIHs) were established to facilitate innovation adoption and digital transformation support for SMEs. However, their effectiveness has been limited: DIHs have not achieved intended outreach to SMEs; their impact on actual business transformation remains modest; and they struggle to attract SMEs and startups to participation. DIHs remain primarily oriented toward universities and large companies rather than serving their intended primary beneficiary, this is, SMEs and startups seeking to understand and adopt digital technologies.

This weakness undermines Europe's capacity to democratise access to continuum technologies. If DIHs were effective, they could serve as local touch points where SMEs could access support in adopting continuum infrastructure, understanding compliance requirements and transitioning business models to continuum capabilities. Without effective DIHs, SMEs lack local support infrastructure and must navigate adoption alone or rely on large vendor support (often hyperscalers). This perpetuates the pattern where large companies advance while SMEs remain stuck in legacy computing models or forced into hyperscaler dependence.

2. Large Initiatives Attracting Large Companies and Universities Rather Than SMEs
Major European initiatives (Gaia-X, IPCEI-CIS, Horizon Europe projects) primarily attract large companies and research universities, not SMEs and startups. This reflects structural features: large initiatives require significant administrative capability to participate; funding mechanisms favour established organisations with grant writing infrastructure; governance structures are designed by large companies for large company participation; and startup voices are marginalised in decision-making.

This weakness is particularly problematic because SMEs and startups are crucial for innovation and ecosystem diversity. When large initiatives exclude SMEs, the result is that European computing continuum development becomes a project of large incumbents rather than emerging innovators. This risks creating continuum solutions that serve large companies' needs while marginalising use cases and applications important to SMEs. Additionally, lack of SME participation in large initiatives means that SMEs do not develop the relationships, understanding and advocacy capacity necessary to influence subsequent initiatives, perpetuating their marginalisation.

3. Fragmentation and Lack of Coordination Among Overlapping Initiatives
Multiple European initiatives address overlapping continuum domains (Gaia-X, IDSA, DOME, SIMPL, IPCEI) but they do not communicate effectively or coordinate objectives. This fragmentation results in duplicated work, incompatible technical standards, competing for limited funding and participant attention, and absence of coherent ecosystem strategy. Individual initiatives pursue their own agendas rather than aligning toward shared continental objectives.

This fragmentation is a critical weakness because it creates confusion for potential participants (which initiative should I join?), undermines credibility with external actors (how can Europe coordinate if Europeans cannot coordinate among themselves?) and dissipates resources across parallel rather than complementary efforts. For companies trying to engage with European continuum initiatives, fragmentation creates burden: participating in multiple initiatives simultaneously is costly; choosing among initiatives creates risk of backing the wrong initiative. This fragmentation is particularly damaging for SMEs who lack resources to monitor and participate in multiple initiatives.

4. Lock-in from Existing US Cloud Contracts in Public Sector

Long-term public sector cloud contracts with US providers (AWS, Azure, Google Cloud) create lock-in that prevents public sector transition to European alternatives. These contracts, backed by substantial financial resources and often including multiple services integrated into public sector operations, create dependencies that extend over years or decades. Public procurement budgets committed to existing US contracts are unavailable for European providers, reducing demand signals that would incentivize European provider development.

This lock-in is consequential because public sector procurement is typically large and stable, enabling infrastructure providers to justify sustained investment. When public budgets are captured by US providers through long-term contracts, European providers lack the demand visibility necessary to justify investment in competing services. Additionally, lock-in prevents experimentation: public sector organisations bound by existing contracts cannot easily shift portions of their workload to European alternatives even if those alternatives become available. Breaking this lock-in requires explicit policy action (e.g., procurement rules favouring European providers or contract restructuring incentives).

5. Low Japanese Participation in Open-Source Software Development

Japanese participation in Free/Libre and Open-Source Software (FLOSS) projects is notably lower than European or US participation. Additionally, Japanese government support for FLOSS infrastructure development may be insufficient relative to support for proprietary software and commercial technologies. This low participation limits collaborative innovation with Japan on open-source foundations that are increasingly central to the computing continuum.

This weakness affects EU-Japan collaboration because open-source development and maintenance is central to European computing continuum strategy. If Japanese actors do not develop significant expertise and engagement with open-source, their ability to contribute to collaborative open-source continuum projects is limited. This creates asymmetry where Europe invests heavily in open-source development but lacks equal Japanese participation to distribute maintenance burdens and share responsibility for critical infrastructure. Addressing this weakness requires not only Japanese policy support for open-source but also cultural shifts in Japanese industry toward viewing open-source as strategic.

6. Weak Capital Markets in Europe Limiting SME Scaling

Europe's capital markets remain insufficient to support SME development at the scale necessary for European companies to compete globally. Venture capital investment is available but in smaller amounts than in US markets; growth-stage funding is harder to access; and private equity is more conservative about supporting high-risk technology ventures. Without adequate capital market support, European SMEs cannot scale to the size necessary to compete with larger non-European competitors or to absorb the investment necessary for continuum technology development.

This structural weakness constrains Europe's ability to develop an ecosystem of medium-sized technology companies that could serve as alternatives to dominant hyperscalers or specialists in niche continuum domains. Instead, European SMEs either remain small specialists or sell to larger non-European acquirers. This creates a missing middle in the European technology ecosystem, too large to remain startup-like but insufficiently capital-supported to achieve global scale. For computing continuum development, the absence of this missing middle means that European infrastructure and services are provided either by large multinational companies (often non-European) or fragmented small companies without resources for quality, reliability and scale.

Funded by the European Union

Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

3.5.4 OPPORTUNITIES

1. Japan's Association with Horizon Europe
An opportunity exists for Japan to formally associate with Horizon Europe, the EU's primary research and innovation funding programme. Japanese association would enable Japanese researchers and companies to participate in Horizon Europe projects, creating collaborative R&D partnerships and shared access to European research infrastructure. This would create evaluable partnerships in research, innovation and technology, as well as enhanced market access within Europe.

This opportunity is significant because it would formalise EU-Japan collaboration on continuum technologies at research and innovation level. Japanese participation in Horizon Europe would bring additional funding, diverse research perspectives and Japanese technology expertise to European continuum research. Additionally, Japanese companies participating in Horizon Europe projects would develop relationships with European partners and gain market knowledge enabling easier transition to European market deployment.

2. EU-Japan Cooperation on Data-Driven Society Standards and Platforms
Cooperation between Europe and Japan on data-driven society standards and platforms, particularly collaboration between Gaia-X (European data infrastructure initiative) and DATA-EX (Japanese data ecosystem initiative), could generate synergies developing a sovereign and secure data ecosystem serving both regions. Rather than each region developing isolated data platforms, collaboration could create interoperable frameworks enabling data flows between regions while maintaining sovereignty and protection.

This opportunity addresses a key computing continuum challenge: how to enable data sharing across regions and organisations while maintaining data protection and sovereignty. European and Japanese collaboration on this problem could produce solutions with broader applicability, potentially becoming standards adopted internationally. For companies in both regions, interoperability between Gaia-X and DATA-EX would enable them to serve customers across both regions without duplicating platform development.

3. Strengthening Collaboration with Japan, South Korea and Extending to Like-Minded Partners
An opportunity exists to systematically strengthen collaboration with Japan and South Korea (countries with demonstrated commitment to technology sovereignty and values-based governance) and extend collaboration to other like-minded countries (Canada, New Zealand, Australia, potentially others). Rather than viewing international collaboration narrowly, Europe can build broader coalitions of countries committed to alternative technology pathways and digital values alignment.

This opportunity addresses the challenge that Europe alone cannot achieve technology scale comparable to US or China. However, coalitions of countries with shared values and complementary capabilities could collectively develop technologies serving substantially larger markets. Such coalitions could coordinate standards, share infrastructure investments and collectively negotiate with dominant global technology providers from position of greater strength. For the computing continuum, a Europe-Japan-Korea-Canada-New Zealand coalition would represent substantial technical capability, large combined markets and shared commitment to values-based digital governance.

4. Coordinating Technical Standards at the EU Level for Edge, IoT and APIs
An opportunity exists to deliberately coordinate technical standards at EU level particularly for network APIs, edge computing interfaces and IoT deployment. This coordination would establish common reference frameworks and promote convergence around open, interoperable standards. Clear European standards would reduce fragmentation, lower

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

integration costs for developers, facilitate scaling across borders and strengthen Europe's influence in international standard-setting bodies.

This opportunity directly addresses fragmentation among initiatives by providing common technical foundation that multiple initiatives can build upon rather than creating competing technical frameworks. When standards are clear and coordinated at EU level, smaller initiatives can focus on application layers rather than reinventing foundational standards. For the computing continuum specifically, coherent technical standards are essential to avoiding fragmentation into incompatible regional systems.

5. Leveraging Japan's Edge/IoT Strategy Development
The IT Promotion Agency (IPA) in Japan is beginning to develop an Edge/IoT strategy, creating opportunity for EU-Japan collaboration on Edge/IoT development and deployment. Japanese interest in NexusForum.EU and European continuum initiatives indicates openness to collaboration. By explicitly engaging Japanese strategy development, Europe can influence Japanese commitment to interoperability and values-based governance in edge/IoT domains.

This opportunity is significant because edge and IoT are foundational to the computing continuum, and Japanese advances in manufacturing, automotive and industrial IoT could complement European capabilities. Joint EU-Japan Edge/IoT strategy could accelerate deployment of both regions' capabilities while establishing coordinated approaches to interoperability and governance.

6. Leveraging Market Dynamics to Promote Interoperability and Reduce US Dependence
Fujitsu's success in securing major Japanese government cloud contracts in competition with US providers indicates that Japanese government is willing to support alternative providers. This market signal can be leveraged to promote broader interoperability and reduce dependence on dominant US providers. By coordinating EU and Japanese procurement policies to favour providers demonstrating interoperability and values alignment, both regions can create market incentives for providers to invest in cross-regional compatibility and shared standards.

This opportunity uses market mechanisms to achieve policy objectives: rather than imposing technical mandates, creating procurement preferences for interoperable solutions incentivizes providers to develop solutions serving multiple regions. For companies, demonstrating interoperability across EU and Japanese infrastructure becomes market advantage. For both regions, coordinated procurement policies multiply the market available to alternative providers, justifying greater investment.

7. Using Industry Advocacy to Advance Interoperability and Prevent Dominant Market Abuse
An opportunity exists to use rest-of-economy advocacy mobilising SMEs, mid-market companies, public sector and industry associations across diverse sectors to press for interoperability and portability requirements that prevent market abuse by dominant technology providers. When diverse industry voices collectively advocate for interoperability, they create political pressure that single companies or small coalitions cannot generate independently.

This opportunity harnesses the natural interests of diverse economic actors in preventing lock-in and maintaining competition. By facilitating coordination among these actors and amplifying their voices, Europe can create political environment where interoperability becomes expected rather than exceptional. This approach is less confrontational than direct regulation and leverages market participants' own interests rather than relying on regulatory mandates.

3.5.5 THREATS

1. Global Competition Without Replicating US or China Dominance
A fundamental threat exists that Europe cannot create computing continuum capabilities competitive with US and China while maintaining democratic governance, rule of law and values-based regulation. Creating innovation ecosystems comparable to US tech hubs requires accepting certain dysfunctions (regulatory arbitrage, tax avoidance, monopolistic concentration) that Europe explicitly rejects. Creating state-level coordination comparable to China requires state direction of private investment and reduced political pluralism that Europe values. This creates a genuine strategic dilemma: Europe cannot compete by copying US or China models without abandoning values that define Europe.

This threat is not easily solved through conventional policy. It requires finding innovations in governance, economics and organisation that create competitive capability without compromising European values. This is possible in principle but requires sustained creativity and willingness to experiment with novel institutional forms, a challenging proposition in consensus-oriented European politics.

2. Dependence on Non-European Technologies if European Alternatives Are Not Developed and Maintained
Despite European efforts to develop continuum alternatives (Gaia-X, IPCEI-CIS, open-source initiatives), significant risk exists that these initiatives will not achieve sufficient maturity, adoption and competitive capability to constitute true alternatives to non-European technologies. If European initiatives remain niche while non-European dominance consolidates, Europe will find itself invested in continuum alternatives that never achieve critical mass, while dependence on non-European technologies actually increases.

This threat reflects the fact that developing technology alternatives requires not only initial research and development but sustained maintenance, continuous innovation and market adoption. Early success does not guarantee long-term viability. Without sustained political commitment and public investment, European initiatives can stall, decline or fragment, leaving Europe technically further behind than before initiatives began.

3. Japanese Isolationism and "Not Invented Here" Attitudes Hindering Collaboration
Japan's historical tendency toward isolationism and preference for domestically developed solutions can hinder international collaboration necessary for EU-Japan partnership. Japanese companies may be reluctant to integrate with European technologies; Japanese government may prefer domestic solutions; and Japanese research communities may see collaboration as diluting intellectual property advantages. Overcoming these attitudes requires not only policy-level agreements but cultural shifts in Japanese industry and government toward viewing international collaboration as strategic advantage rather than threat.

This threat reflects genuine cultural and institutional differences between Europe and Japan that cannot be overcome through policy alone. Addressing this threat requires long-term relationship building, demonstrated mutual benefits and explicit management of intellectual property and credit attribution concerns.

4. Competing with Free or Low-Cost Entry-Level Solutions
A significant threat exists that emerging technologies and solutions, whether developed in other regions, by dominant global providers offering loss-leader pricing or by innovative startups in less-regulated jurisdictions, will undercut European alternatives at entry level. Customers evaluating computing continuum solutions often choose based on immediate cost rather than long-term considerations like vendor independence or data control. This cost-based competition threatens European alternatives that must sustain long-term maintenance and support.

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

This threat requires addressing not only through superior quality or capabilities but through customer education and value proposition communication. Customers must understand that data control, interoperability and vendor independence have economic value, not merely compliance or values-based value. This is a market development challenge requiring sustained messaging and customer engagement.

5. Market Dominance by Hyperscalers Extending to Edge and IoT Domains
A critical threat exists that existing cloud hyperscalers will extend their dominance into edge computing and IoT domains, leveraging their existing customer relationships, financial resources and integrated service capabilities. Hyperscalers have demonstrated capability to suppress or integrate competing services; they can offer edge and IoT services integrated with their existing cloud platforms, creating advantage over standalone European competitors. If hyperscalers achieve dominance in edge and IoT before European alternatives mature, European alternatives may never achieve critical mass.

This threat is urgent because the computing continuum depends on integrated edge, cloud and IoT capabilities. If hyperscalers control the integration layer, they effectively control the continuum despite fragmentation at individual component level. Addressing this threat requires ensuring European alternatives achieve sufficient functionality and market adoption before hyperscaler dominance becomes insurmountable.

6. CRA Liability Concerns Chilling FLOSS Development
The Cyber Resilience Act's provisions create concerns among FLOSS developers and organisations about potential liability if their software is used in critical infrastructure and subsequently found to have security vulnerabilities. This liability uncertainty is chilling investment in open-source development: developers and organisations are reducing participation in critical projects, some are ceasing maintenance, and NPOs and public sector organisations are becoming cautious about FLOSS adoption. This dynamic directly undermines the open-source foundation that European computing continuum strategy depends upon.

This threat reflects regulatory design that had unintended consequences. The CRA was intended to improve cybersecurity, but its application to open-source created perverse incentives that reduce security-critical infrastructure vitality. Addressing this threat requires regulatory refinement to clarify FLOSS liability frameworks and provide safe harbours for good-faith open-source development.

3.5.6 SYNTHESIS

Factor 5 characterises a landscape where Europe possesses institutional capacity for large-scale coordination (demonstrated by IPCEI-CIS and multisectoral initiatives), emerging strategic partnerships with aligned international actors (Japan, potentially others) and mechanisms for continent-level collaboration. However, significant weaknesses persist: fragmentation among overlapping initiatives that fail to coordinate, ineffectiveness of support mechanisms for SMEs and startups, lock-in from existing non-European cloud contracts and insufficient capital markets to support SME scaling. Additionally, efforts to build European alternatives to dominant technology providers occur in context of global competition that favours consolidation over fragmentation and of geopolitical uncertainty.

Concrete opportunities exist to deepen international partnerships (Japan association with Horizon Europe, EU-Japan standards collaboration, broader coalitions with like-minded countries), to improve internal European coordination (clarifying standards, strengthening SME inclusion), and to leverage market dynamics and industry advocacy to advance interoperability.

Threats, including hyperscaler dominance extension into edge/IoT, regulatory chilling effects on open-source and inability to compete without compromising European values, underscore the need for sustained, coordinated strategy that sustains political will over years despite geopolitical uncertainties.

The central strategic question for Factor 5 is whether Europe can create collaboration mechanisms and international partnerships sufficiently robust to maintain momentum toward alternative technologies despite external pressures toward consolidation and dominance, while maintaining European values-based governance and democratic pluralism. This requires both external partnerships with like-minded actors and internal coordination that overcomes European fragmentation, a dual challenge requiring sustained political commitment.

3.6 SWOT Factor 6: Industry Participation

3.6.1 Context

Factor 6 focuses on the engagement, capacity and strategic alignment of European industry from large technology and telecommunications companies to SMEs and startups. Industry participation determines whether technological capabilities developed through research translate into competitive products, services and market leadership. Without sustained industry engagement and participation, continuum technology remains confined to research environments and policy discussions rather than driving economic growth and digital transformation across sectors.

Europe possesses strong financial commitment toward computing continuum development, evidenced by substantial public and private investment in IPCEI-CIS and complementary initiatives. Over 100 industrial partners from 12 Member States are engaged in IPCEI-CIS alone, bringing diverse expertise and market perspectives. Europe maintains world-leading industry players in telecommunications (Ericsson, Nokia), automotive (Volkswagen, BMW, others) and industrial sectors that are significant potential beneficiaries of continuum technologies. However, significant weaknesses persist: limited support and resources for SMEs within initiatives; emphasis on research-driven approaches disconnected from practical industry application; weak capital markets restricting SME scaling; unclear regulatory scope creating compliance uncertainty for companies; and short-term business pressures forcing SMEs toward survival strategies rather than transformation.

The central challenge for industry participation is ensuring that continuum development serves industry needs and translates into practical business applications rather than remaining academic exercise. This requires mechanisms to include SME voices in continuum strategy, creating accessible pathways for SMEs to participate in initiatives, and establishing clear regulatory frameworks that enable rather than constrain industry innovation.

3.6.2 STRENGTHS

1. Strong Financial Commitment Toward Computing Continuum Development
Europe demonstrates strong financial commitment toward computing continuum technologies through substantial public and private investment. IPCEI-CIS alone mobilises €2.6 billion in investment; Horizon Europe allocates billions for digital technology research; and Member States commit additional funding through national programmes. This financial commitment signals political and business confidence in continuum strategic importance and provides resources for sustained development.

This financial commitment is significant because developing competitive technologies requires years of investment before commercial viability. Public funding commitment provides stability that private markets alone cannot guarantee, enabling companies and researchers to make long-term investment decisions. For SMEs and startups, public funding availability (through Horizon Europe, national programmes, venture capital) provides alternative to internal cashflow constraints that otherwise limit experimentation with emerging technologies. The scale of commitment also signals to international partners (particularly Japan) that Europe is serious about continuum development, potentially justifying reciprocal international investment.

2. Industry Involvement Ensuring Diverse Perspectives and Expertise

The involvement of over 100 industrial partners from 12 Member States in IPCEI-CIS ensures that industry perspectives and expertise shape continuum development from early stages. Large companies contribute technical expertise and manufacturing capability; suppliers contribute component expertise; service providers contribute market understanding. This industrial diversity prevents research from becoming disconnected from practical requirements and ensures that solutions address genuine industry needs.

This industrial involvement is particularly important for SMEs because it creates opportunities for SME participation in large initiatives and access to knowledge, standards and technologies developed at initiative level. When SMEs participate in consortium projects, they gain insights into emerging technologies, establish relationships with potential partners or customers and develop capabilities for next-generation services. For the continuum specifically, industrial involvement ensures that technical architecture decisions reflect practical deployment requirements across diverse sectors rather than abstract research concerns.

3. Strategic Commitment to Technological Sovereignty

Europe and its industry actors are explicitly committed to technological sovereignty, maintaining European control over essential technologies rather than depending on non-European providers. This commitment reflects both geopolitical reality (recognition that technology dependence creates political vulnerability) and business opportunity (recognition that technological alternatives create market opportunities). Industry participation in sovereignty initiatives is driven not only by public funding incentives but by genuine business recognition that European market for continuum technologies will favour European providers meeting European regulatory and governance standards.

This commitment to sovereignty is a strength because it aligns public policy and industry incentives. When industry genuinely believes that European technology development is strategically important and commercially viable, they invest accordingly. This alignment reduces the need for government mandates or artificial incentive structures; industry self-interest drives participation. For SMEs and startups, this alignment means that European continuum opportunities are not marginal niches but represent core strategic directions for larger companies and investors.

4. Strong Industry Players Positioned as Major Continuum Beneficiaries

Europe has world-leading industry players in sectors that are major potential beneficiaries of computing continuum technologies: automotive (Volkswagen, BMW, Daimler), telecommunications (Ericsson, Nokia, Telefónica, Deutsche Telekom), industrial manufacturing (Siemens, Philips), energy (Shell, BP) and chemicals (BASF, Bayer). These companies are increasingly recognising that Industry 4.0, smart manufacturing, predictive maintenance and supply chain optimisation depend fundamentally on continuum capabilities. As these companies' digital transformation accelerates, demand for continuum infrastructure, services and integration expertise increases, creating economic incentives for European continuum provider development.

This industrial strength provides continuum development with an anchor customer base capable of justifying sustained investment in continuum solutions. When Volkswagen commits to electric vehicle and autonomous driving development, it creates demand for edge computing, real-time data processing and distributed decision-making that drives investment in continuum technologies. Similarly, when energy companies pursue digital transformation of grid management and renewable integration, they create demand for edge computing and IoT infrastructure. For SMEs and startups, these anchor customers provide market opportunities and potential pathways to scaling.

3.6.3 WEAKNESSES

1. Research-Driven Approach Potentially Disconnected from Practical Industry Needs
While research investment is necessary for frontier technologies, there is risk that emphasis on research-driven innovation may disconnect technology development from practical industry applications. Large research programmes, particularly Horizon Europe projects, emphasise novel technical approaches and advance scientific knowledge but may not optimise for practical deployment, cost-effectiveness or business model viability. Companies attempting to commercialise research outputs often discover that research results do not directly address industry-prioritised problems or that integration into production systems requires extensive additional development.

This weakness constrains industry participation because companies unwilling to invest years translating research into commercial products become discouraged from research collaboration. SMEs particularly suffer because they lack internal R&D capacity to invest in research-to-production translation. The result is that promising research outputs remain confined to academic environments and do not transition into commercial products benefiting end-users. For the continuum specifically, this means that sophisticated research on continuum architectures and technologies may not result in practical continuum solutions that companies can deploy.

2. Limited Support and Resources for SMEs within Initiatives
Although European initiatives theoretically include SMEs, practical support and resources for SME participation remain limited. Large initiatives are designed by and for large companies and research institutions; SMEs must adapt their operations to match initiative requirements rather than initiatives adapting to SME constraints. SME participation is often limited to subcontractors to large company leads rather than as strategic partners. Funding mechanisms favour large consortia where administrative overhead is justified by project scale; small projects serving SME-specific needs struggle to secure funding.

This weakness systematically disadvantages SMEs despite their importance to innovation and market competitiveness. SMEs are pushed toward either: (a) remaining small specialists without resources for continuum scale, or (b) seeking acquisition by larger companies, resulting in consolidation rather than thriving independent SME ecosystem. For the continuum, this means that innovation opportunity space addressable only by nimble SMEs may remain unexploited, and European SMEs may fail to develop the capabilities necessary to compete as continuum matures into commercial markets.

3. Weak Capital Markets Insufficient to Support SME Development
Europe's capital markets remain insufficient to support SME development at scales necessary for European technology companies to achieve global significance. Venture capital is available but in smaller amounts than US markets; growth-stage funding is harder to access; and private equity is more conservative about technology sector risk than in US markets. Without adequate capital market support, European SMEs remain constrained in size and reach.

This weakness has cascading effects: SMEs cannot scale to sizes where they can employ large development teams, conduct extensive market validation or build global sales organisations; talented engineers and founders are drawn to US technology companies or non-European competitors where capital is more available; and continuum technology ecosystem remains fragmented across numerous small players rather than consolidating into medium-sized companies capable of sustained innovation. For the continuum specifically, capital weakness means that promising continuum startups are likely to be acquired by non-European companies or to fail rather than achieving independent viability.

4. Lack of Clarity and Regulatory Uncertainty Challenging for Companies
Regulatory scope and application remain unclear for many rules affecting computing continuum companies, particularly rules around data protection, cybersecurity, AI governance and product liability. This regulatory uncertainty creates compliance costs and delays as companies attempt to understand obligations and implement compliance mechanisms. For companies developing continuum technologies incorporating AI, open-source software or distributed processing, regulatory uncertainty compounds compliance challenges.

This weakness is particularly damaging for fast-moving startups and SMEs that lack regulatory expertise and cannot afford extended compliance discussions with authorities. Regulatory uncertainty forces them toward conservative interpretations (implementing stricter compliance than actually required) or toward non-compliance due to inability to understand requirements. The result is either higher costs stifling innovation or non-compliance creating legal exposure. For the continuum specifically, regulatory uncertainty particularly affects companies developing edge AI, open-source integration or new data processing models where regulatory boundaries remain evolving.

5. Short-Term Business Pressures Forcing SME Survival Strategies
SMEs face continuous pressure to achieve short-term profitability, creating tension with longer-term investment necessary for continuum technologies. SMEs often cannot afford to invest significantly in emerging continuum technologies when doing so reduces near-term revenue. This forces SMEs toward "survival mode" business strategies focused on maintaining current operations rather than transformation toward continuum capabilities. The result is that many SMEs remain locked in legacy technology modes despite recognising that continuum transition is strategically necessary.

This weakness is structural to SME economics and difficult to address through policy alone. SMEs require either access to capital enabling them to invest in transformation without sacrificing profitability, or business models and solutions making continuum adoption financially sensible without requiring subsidy. Without addressing this economic reality, continuum adoption by SMEs remains limited despite policy encouragement.

3.6.4 OPPORTUNITIES

1. Automotive Industry Digitalization Through Computing Continuum
The automotive industry, a European strength and global competitor, faces fundamental transformation toward electric vehicles, autonomous driving and connected car capabilities. These transformations depend fundamentally on computing continuum technologies: edge computing in vehicles, cloud processing of driving algorithms, IoT sensor networks and real-time data processing. The development of standardised data formats and exchange protocols enabling seamless communication between vehicle components and external systems can boost automotive competitiveness and accelerate transition to smarter, more sustainable mobility.

This opportunity is significant because it provides anchor market for continuum technology development. When automobile manufacturers commit to continuum-enabled vehicles, they create demand for edge computing platforms, IoT connectivity, cloud processing services and data management infrastructure. European suppliers can develop continuum solutions targeting automotive needs, then extend solutions to other sectors. Additionally, automotive leadership in continuum drives investment in related skills (autonomous systems, sensor networks, real-time processing) that benefit broader technology ecosystem. For SMEs and startups, automotive provides clear market applications and potential customers for continuum services.

2. Supporting European Providers of Telecommunications Equipment and Software
An opportunity exists to systematically support European telecommunications equipment and software providers through procurement preferences, regulatory streamlining and targeted R&D funding. European providers (Ericsson, Nokia and others) have capabilities in 5G/6G, edge computing and network virtualisation; supporting their continued investment ensures that European industry maintains advantages in telecommunications infrastructure. Initiatives like deployment of 10,000 edge nodes across Europe can strengthen technological autonomy while creating market demand for European equipment and software.

This opportunity is important because telecommunications infrastructure is foundational to computing continuum. European leadership in telecommunications equipment ensures that continuum infrastructure is built using European technologies meeting European standards. For SMEs and startups, European telecommunications provider strength creates ecosystem of suppliers, integration partners and service providers that generate employment and economic activity. Supporting European telecommunications providers is thus supporting entire ecosystem that depends on them.

3. Strengthening European Semiconductor Industry
An opportunity exists to significantly strengthen Europe's semiconductor industry through a comprehensive EU Semiconductor Strategy based on multiple pillars: funded innovation labs developing next-generation chip design and manufacturing; incentives for fabless companies (chip designers without their own manufacturing) to develop designs for European manufacturing; funding for chip fabrication facilities (fabs) focused on strategic segments (automotive, AI, chiplets, network equipment); support for innovation in conventional and chiplet technologies; and funding for advanced materials and 3D packaging technologies.

This opportunity addresses a fundamental vulnerability: European dependence on non-European semiconductor suppliers. A stronger European semiconductor industry enables European companies to design and manufacture chips meeting European requirements, reduces supply chain vulnerability and positions Europe as semiconductor technology leader. For the continuum specifically, semiconductors are foundational; stronger European semiconductor capabilities enable European-designed edge devices, IoT sensors and cloud infrastructure rather than depending on designs from non-European vendors.

4. Industry Commitment to Interoperability and Open Standards
An opportunity exists for European industry to make explicit commitment to interoperability and open standards as competitive differentiation. Companies adopting open-source software and commitment to interoperability can position themselves as alternatives to proprietary, lock-in vendor approaches. Industry commitment to interoperability can enhance collaboration and integration across different technologies and platforms. Such commitment signals to customers (particularly public sector and regulated industries) that these providers prioritise customer interests over vendor lock-in.

This opportunity leverages market dynamics where customers increasingly recognise value of interoperability and are willing to prefer providers demonstrating commitment to it. When European industry collectively commits to interoperability, it creates competitive advantage for European companies in markets valuing independence and avoiding lock-in. For SMEs and

Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

startups, explicit industry interoperability commitment creates assurance that their solutions can integrate with broader ecosystem rather than being trapped in proprietary platforms.

5. Leveraging Public Procurement and European Value Chains
An opportunity exists to deliberately use public procurement to support European technology providers and strengthen European value chains. By procurement preference policies favouring European providers meeting European standards and demonstrating supply chain resilience, public sector can create sustained demand enabling European providers to justify investment in innovation and scaling. Additionally, by coordinating procurement at European level rather than fragmenting across Member States, public sector can create scale economies enabling European providers to compete with larger global competitors.

This opportunity converts public procurement into strategic tool rather than purely cost-minimisation activity. While procurement-based approach cannot single-handedly create competitive industries, combined with R&D support and regulatory environment enabling innovation, strategic procurement can tip scales toward European provider development. For SMEs and startups, predictable public procurement demand provides business foundation enabling investment in growth and innovation.

6. Enhancing EU Computing Infrastructure Accessibility for Businesses
An opportunity exists to enhance European computing infrastructure (data centres, edge facilities, AI processing capacity) and make it more accessible to businesses, particularly SMEs. By developing business models where public computing infrastructure developed through research investment (Euro-HPC, AI Factories) is made available to commercial users on reasonable terms, Europe can democratise access to advanced computing resources. SMEs lacking resources to build their own infrastructure can access continuum-grade computing capacity without depending on hyperscalers.

This opportunity addresses the fundamental inequality where large companies can afford to build or procure advanced infrastructure while SMEs cannot. By making public infrastructure accessible, Europe levels the competitive playing field. For the continuum specifically, making Euro-HPC and similar facilities accessible to commercial users ensures that European companies have access to computing resources necessary to develop and deploy continuum applications.

7. Making Computing Infrastructures Easier and More Open for Business Use
An opportunity exists to systematically simplify access to European computing infrastructure for commercial use, reducing barriers to adoption. This includes: simplifying procurement and service agreements for companies to use public computing facilities; establishing clear, transparent pricing models; providing technical support for companies to understand how to leverage infrastructure effectively; and removing administrative burdens that make public infrastructure less attractive than commercial alternatives.

This opportunity addresses practical barriers that often make public infrastructure less attractive to companies than proprietary commercial alternatives despite policy intentions. When public infrastructure has simpler terms, clearer pricing and better support than commercial alternatives, companies adopt it naturally. For the continuum specifically, making European public infrastructure genuinely attractive to commercial users ensures that European continuum deployment benefits from publicly-supported infrastructure rather than depending entirely on private commercial alternatives.

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

3.6.5 THREATS

1. Dependence on Foreign Vendors for Critical Technologies
Europe heavily depends on foreign vendors for critical technology components: cloud services dominated by US providers; mobile phone operating systems (Apple iOS, Android/Google); semiconductor manufacturing capacity concentrated in non-European regions; and increasingly, AI model development and deployment. This dependence creates strategic vulnerability: if foreign vendors restrict technology access for geopolitical or commercial reasons, European industry suffers direct impact. Additionally, dependence means that technology development trajectories are determined by foreign vendors rather than European companies.

This threat is structural and cannot be entirely eliminated because achieving 100% self-sufficiency in all technologies is economically unrealistic. However, reducing dependence in strategically critical domains (cloud, semiconductors, AI) is necessary for technological autonomy. Addressing this threat requires deliberate public and private investment in European alternatives in critical domains, even when such investment is economically suboptimal by short-term metrics.

2. Fierce Global Competition Particularly from US and China
Intense global competition, particularly from US technology giants and Chinese state-backed technology companies, represents a major threat to European technology competitiveness. US companies have advantages of large unified market, deeper capital markets and established network effects in deployed systems. Chinese companies have advantages of state financial support, large domestic market and less restrictive regulatory environment enabling rapid experimentation. European companies face competition from both directions while operating within more constrained financial, regulatory and market conditions.

This threat is not new but has accelerated as technology competition has intensified. Creating competitive environment without replicating US or China situations, without sacrificing European values around regulation, labour rights, and environmental protection, is genuine strategic challenge. Addressing this threat requires Europe to find novel competitive advantages rather than competing on same dimensions as US and China.

3. Regulatory Fragmentation and Lack of Member State Harmonisation
Fragmentation and lack of regulatory agreement among EU Member States create significant challenges for industry. Different Member States interpret common EU regulations differently; national regulations diverge in ways creating compliance complexity; and enforcement varies significantly. This fragmentation is particularly problematic for startups and SMEs needing to operate continent-wide. The startup environment in Europe is challenging due to regulatory mismatches making it difficult for startups to operate continent-wide; lack of tax harmonisation acts as structural barrier to development of unified European technology ecosystem.

This threat is self-inflicted through European federal structure where Member States retain authority over many regulatory domains. Unlike US where federal regulation provides uniform framework or China where central government provides unified regulation, Europe must achieve harmonisation through negotiation and consensus. When Member States prioritise different objectives or protect local companies through regulatory barriers, fragmentation persists. This fragmentation is structural threat to European industry competitiveness because it prevents consolidation into companies of sufficient scale to compete globally. Addressing it requires political will among Member States to prioritise European competitiveness over national protection.

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

3.6.6 SYNTHESIS

Factor 6 characterises a landscape where Europe possesses strong financial commitment to continuum development, engagement of major industry players in world-leading sectors (automotive, telecommunications, manufacturing) and explicit strategic commitment to technological sovereignty. However, significant weaknesses persist: limited support for SMEs despite their innovation importance; research-driven approaches disconnected from practical business applications; weak capital markets restricting company scaling; regulatory uncertainty creating compliance burdens; and structural economic pressures forcing SMEs toward survival rather than transformation.

Concrete opportunities exist to leverage anchor customers (automotive digitalization), to support critical industrial sectors (semiconductors, telecommunications), to use public procurement as strategic tool and to democratise access to computing infrastructure. These opportunities can drive industry participation and translate continuum research into commercial applications. Threats, including foreign vendor dependence, intense global competition and regulatory fragmentation, underscore need for sustained, coordinated industrial policy that supports European industry development while maintaining European competitive and ethical standards.

The central strategic question for Factor 6 is whether Europe can create conditions enabling European industry, particularly SMEs, to develop competitive continuum businesses, overcoming structural disadvantages relative to better-capitalised, less-regulated competitors. This requires addressing not only technology and regulation but fundamental economic conditions: capital market access, market scale, business model viability and talent availability. Without addressing these economic conditions, even excellent technology will not translate into industry competitiveness.

Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

4 CRITICAL GAPS: BARRIERS TO COMPUTING CONTINUUM LEADERSHIP

The comprehensive SWOT analysis across six foundational factors reveals that Europe's path to computing continuum leadership is obstructed by 14 critical gaps representing systemic weaknesses across technological, infrastructural, governance and operational dimensions. Addressing these gaps is essential for transforming European continuum capabilities from fragmented initiatives into coherent continental strategy.

GAP 1: Technological Sovereignty Challenges
Slow adoption of advanced technologies, limited trust in AI and data security, and dependence on non-EU solutions undermine the EU's technological autonomy.

European companies and public institutions remain dependent on non-European AI systems, cloud platforms and critical technologies. Trust in European solutions is lower than in non-European alternatives despite European regulatory excellence. Limited domestic capacity in cutting-edge domains (advanced AI, quantum computing, neuromorphic systems) forces continued reliance on external providers.

GAP 2: Fragmented Infrastructure Ecosystem
Disconnected edge, cloud, and IoT resources hinder the creation of a trusted, federated computing continuum across Europe.

Gaia-X and related initiatives represent conceptual excellence but practical fragmentation persists. Data centres remain disconnected; edge resources are dispersed without unified management; IoT deployments lack common standards. Multiple overlapping initiatives (SIMPL, DOME, IDSA) create confusion without achieving integration.

GAP 3: Regulatory Complexity for SMEs
Fragmented and burdensome regulations, lack of harmonization, and high compliance costs limit the growth and innovation capacity of SMEs and startups.

SMEs navigate 27 different regulatory interpretations; compliance requires substantial legal and technical resources unavailable to small companies; regulatory uncertainty in emerging domains (edge AI, distributed systems) forces conservative implementations or non-compliance. Startup environment is particularly challenging due to regulatory mismatches.

GAP 4: Low Confidence in EU Cloud Providers
Limited trust in EU-based cloud solutions contributes to skepticism about Europe's ability to compete with global hyperscalers.

European cloud providers lack the reputation, integrated service offerings and global reach of hyperscalers. Enterprise customers often view European providers as inferior alternatives rather than solutions aligned with European values. European cloud providers struggle to achieve scale necessary for competitive pricing.

GAP 5: Barriers to Cross-Border Data Sharing
Legal, technical, and organizational obstacles to accessing and sharing data across borders restrict the development of Common European Data Spaces and data-driven innovation.

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

Data localisation requirements, unclear data governance, technical incompatibilities and organisational hesitation prevent effective cross-border data sharing. Common European Data Spaces remain largely conceptual rather than operational. SMEs struggle to access data necessary for innovation.

GAP 6: Weak Open-Source Ecosystem
Limited resources and skills in open-source software, coupled with low engagement from large enterprises, slow down innovation and adoption.

European open-source projects lack sustainable funding; shortage of skilled open-source developers; corporate engagement in open-source governance remains minimal; Cyber Resilience Act liability concerns are chilling open-source development. Open-source remains culturally peripheral in many European organisations.

GAP 7: SME Dependence on Non-EU Hyperscalers
Heavy reliance on foreign cloud providers and fragmented European infrastructure reduce digital sovereignty and competitiveness.

70%+ of European SMEs rely on non-European cloud providers; European alternatives lack integrated service ecosystems; cost advantages of hyperscalers (global scale) disadvantage European alternatives; regulatory uncertainty prevents SME adoption of European solutions.

GAP 8: Infrastructure Fragmentation and Energy Costs
Disjointed HPC, digital, and networking infrastructures, high energy costs, and lack of a unified strategy for 5G/6G and fiber deployment weaken Europe's competitiveness.

Data centre markets fragmented across Member States; 5G/6G deployment inconsistent; fibre deployment incomplete; energy costs 2-3x higher than US/Asia; no unified strategy coordinating infrastructure investments. Infrastructure lacks scale economies available in unified markets.

GAP 9: Lack of Quantum-HPC Integration Strategy
The absence of a clear roadmap for integrating quantum computing with HPC threatens Europe's leadership in hybrid computing models.

Quantum computing development proceeds in isolation from HPC infrastructure; no strategy for integrating quantum capabilities into production continuum systems; European quantum leadership may not translate into practical computing advantage without HPC integration.

GAP 10: Ineffective Coordination of Strategic Initiatives
Overlapping goals, unclear business objectives, and weak SME engagement in initiatives like Gaia-X, IDSA, and IPCEI reduce their overall impact.

Multiple initiatives pursue similar objectives with insufficient coordination; governance structures unclear; business models for initiatives not articulated; SME participation limited; results fragmented rather than integrated. European observers and participants struggle to understand how initiatives fit together.

Funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

GAP 11: Limited SME Participation in Global Ecosystems
Dependence on non-EU platforms and low involvement in international digital ecosystems weaken Europe's global positioning.

European SMEs primarily engage with non-European platforms; limited participation in global standards bodies; few European SMEs operate globally; brain drain as entrepreneurs relocate to non-European ecosystems.

GAP 12: Funding Gaps and SME Vulnerability
Short-term financial pressures and limited access to growth capital prevent SMEs from scaling and building resilience.

European venture capital 5-10x smaller than US; growth-stage funding limited; private equity conservative on technology; SMEs struggle to fund transformation toward continuum; survival pressures prevent strategic investment.

GAP 13: Vendor Lock-In Risks
High dependence on foreign technology vendors increases the vulnerability of European SMEs and reduces strategic flexibility.

European companies locked into non-European vendors through contracts, data dependence, and technical lock-in; contractual data portability limited; switching costs prohibitive; competitive alternatives limited.

GAP 14: Semiconductor Supply Chain Weaknesses
Reliance on non-EU semiconductor suppliers and underdeveloped capital markets hinder SME competitiveness in advanced technologies.

European semiconductor design and manufacturing concentrated in few companies; limited fabs for advanced nodes; dependence on non-European suppliers for critical components; European chip designer ecosystem weak.

Note: The 14 critical gaps identified represent a preliminary taxonomy derived from the comprehensive SWOT analysis conducted during 2025. While this gap synthesis provides a structured foundation for understanding Europe's continuum challenges, it is important to note that this is an intermediate analytical output. The primary deliverable of the NexusForum project will be the policy recommendations and strategic actions that build on this gap analysis and are aligned with the Strategic Destinations for Europe's AI Computing Continuum Ecosystem.

Funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

5 CONCLUSION

The Computing Continuum represents both a strategic opportunity and an urgent challenge for Europe. Europe possesses significant strengths such as research excellence, regulatory sophistication, commitment to values-based digital governance, and emerging infrastructure initiatives. However, realising continuum leadership requires decisively addressing critical gaps that currently prevent Europe's fragmented strengths from combining into a unified continental strategy.

These gaps are not primarily technological, European technologists can develop cutting-edge continuum solutions. Rather, gaps are systemic: fragmented governance prevents coordination, regulatory complexity discourages innovation, insufficient capital markets limit company scaling, and infrastructure fragmentation prevents achieving continental scale. Addressing gaps requires both political will and institutional innovation and technical capability.

Europe's distinctive pathway to continuum leadership is neither replicating US technology dominance nor adopting Chinese state direction. Rather, Europe should develop federated, open and interoperable continuum infrastructure reflecting European values: respecting individual rights, enabling democratic oversight of technology, ensuring data control and ethical governance. This European approach will not appeal universally, but it will appeal strongly to customers and societies valuing transparent, trustworthy and values-aligned technology.

Success requires moving from rhetorical commitment to operational action. Political leaders must demonstrate willingness to commit sustained resources (billions of euros annually for years), to prioritise European Continuum development, and to coordinate action across Member States despite varied national interests. Industry must shift from relying on non-European providers to committing to European alternatives, from treating open source as peripheral to considering it central infrastructure, and from pursuing short-term profits to building long-term competitive advantage.

The window for decisive action is limited. Computing continuum infrastructure is being deployed globally now; early-stage decisions establish path dependencies constraining future options; competitors are advancing rapidly. Delayed European action will require more expensive remediation later. If Europe can address the gaps decisively, Europe can achieve computing continuum leadership distinctive from and competitive with dominant global players. If these gaps cannot be addressed, Europe risks technological dependence undercutting digital autonomy and economic competitiveness for decades.

The choice is before European leadership: invest decisively now in addressing these gaps, or accept technological dependence and cede control of essential infrastructure to non-European actors. The Computing Continuum is too important to European future to allow it to proceed by default, carried along by external dynamics. Europe must seize the initiative.

Funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI