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

NEXUS FORUM.EU

SWOT Analysis regarding Factor 4:

INFRASTRUCTURES & CONNECTIVITY

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.

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

1 Context

Factor 4 “Infrastructures & Connectivity” 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 physical substrate and connectivity structure that determine whether continuum architectures can function at scale and across borders.

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.

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 STRENGTHS

2.1 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 such as *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 investments creates a distinctive European approach to infrastructure, geared towards interoperability, decentralisation and values-based sovereignty, rather than dependence on a single provider.

2.2 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.

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 virtualisation, ensuring that European infrastructure evolves with cutting-edge technologies rather than remaining dependent on non-European vendors' product roadmaps.

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

2.3 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.

2.4 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 the development of data spaces (common standards and frameworks for data sharing across organisations and sectors) creates a distinctive governance approach for 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.

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 WEAKNESSES

3.1 SME Dependence on Non-European Hyperscalers for Digital Infrastructure

SMEs across Europe rely on global hyperscalers such as AWS, Microsoft Azure and 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.

3.2 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.

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 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 non-competitiveness: 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.

3.4 Fragmented Digital Infrastructure and Inconsistent 5G/6G and Fibre Investment

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.

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 OPPORTUNITIES

4.1 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 manage shared research facilities, can provide capabilities that SMEs can access through service models, eabling them to effectively access computing capacity without having to build their own infrastructure or rely 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.

4.2 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 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.

4.3 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

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

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.

4.4 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.

4.5 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.

5 THREATS

5.1 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.

5.2 Global Geopolitics and US Policy Uncertainty

Geopolitical tensions between the EU and non-European powers, particularly uncertainty regarding US administration’s policies on European digital autonomy, pose a threat to the development of European infrastructure. 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.

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

6 Synthesis

Factor 4 “Infrastructures and Connectivity”, 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 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.

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