

EuroStack Project Response to the Call for Evidence "2025 Strategic Foresight Report"

Author: Stefane Fermigier (sf@fermigier.com)

Date: 25 Feb. 2025

Version: 1.0

To the Secretariat-General of the European Commission,

This submission provides evidence-based input to the 2025 Strategic Foresight Report, focusing on long-term EU resilience, from the perspective of the EuroStack Project (<https://euro-stack.com>). We believe that achieving genuine digital sovereignty, built upon Open Source principles and a thriving European ecosystem, is *essential* for overall EU resilience. Our response is structured around the key questions posed in the Call for Evidence, drawing upon the comprehensive [EuroStack Vision](#) and [Manifesto](#).

1. Scope: Main Challenges and Strengths for Long-Term EU Resilience

Main Challenges

- **Over-Reliance on Non-European Tech Giants:** The dominance of non-European hyperscalers in cloud computing, data infrastructure, and digital platforms represents a critical vulnerability. This reliance creates economic dependence, risks data sovereignty (due to extraterritorial laws like the US FISA or CLOUD Act), undermines European competitiveness, and limits Europe's ability to shape its digital future according to its values. The failure of Gaia-X exemplifies the dangers of a flawed approach to addressing this challenge.
- **Fragmented Digital Ecosystem:** A lack of cohesive, interoperable European digital infrastructure hinders innovation, collaboration, and the ability of European businesses, particularly SMEs, to compete globally.
- **Cybersecurity Threats:** The increasing sophistication and frequency of cyberattacks, including those targeting critical infrastructure, pose a significant threat to EU resilience. A reliance on proprietary, closed-source systems exacerbates these risks due to limited transparency and auditability.
- **Skills Gap:** A shortage of skilled professionals in areas like open-source technologies, cloud computing, and cybersecurity hinders the development and deployment of sovereign digital solutions.
- **Lack of Strategic Investment:** Insufficient and strategically misdirected investment in European-grown open-source technologies and SMEs limits the growth of a competitive and resilient digital ecosystem.

Strengths

- **Strong European Values:** The EU's commitment to democracy, privacy, transparency, and inclusivity provides a solid ethical foundation for building a resilient digital future.
- **Vibrant Open Source Community:** Europe has a thriving Open Source community and a growing number of innovative SMEs developing sovereign digital solutions.
- **World-Leading Research and Innovation:** European research institutions and universities are at the forefront of many key technologies, providing a strong basis for building indigenous capabilities.

- **Regulatory Framework (GDPR):** The GDPR provides a strong framework for data protection and serves as a model for other regions.
- **Growing Awareness of Digital Sovereignty:** There is increasing awareness among policymakers and businesses of the importance of digital sovereignty for long-term resilience.

2. Imagine 2040: A Resilient EU in 2040

A resilient EU in 2040 would be characterized by:

- **Digital Sovereignty:** Control over its critical digital infrastructure, including cloud computing, data centers, identity systems, and payment systems, all built upon a foundation of open standards and Open Source software (the "EuroStack"). This reduces reliance on non-European providers and ensures that European data is governed by European laws and values.
- **Thriving Digital Ecosystem:** A robust, competitive, and innovative ecosystem of European businesses, particularly SMEs, providing a diverse range of digital solutions. Public procurement policies actively favor these businesses and open-source projects.
- **Data-Driven Innovation:** Secure and interoperable data sharing frameworks enable data-driven innovation across all sectors, while respecting privacy and data sovereignty.
- **Cyber-Resilient Infrastructure:** Digital infrastructure is designed and operated with security as a core principle, leveraging the transparency and auditability of open source to mitigate cyber threats. A Zero Trust Architecture is the default.
- **Skilled Workforce:** A highly skilled workforce, equipped with the knowledge and expertise to develop, deploy, and maintain sovereign digital solutions. Open Source technologies are a core component of education and training at all levels.
- **Sustainable Digital Infrastructure:** Digital infrastructure is designed and operated with a focus on energy efficiency and environmental sustainability, contributing to the EU's climate goals.

3. Society and Generations: Ensuring a Resilient Society and Fairness

- **Digital Inclusion:** Ensure access to digital technologies and opportunities for all citizens, regardless of their location, background, gender, or socioeconomic status. This includes bridging the digital divide and promoting digital literacy.
- **Ethical AI:** Develop and deploy AI systems that are fair, transparent, and accountable, adhering to European ethical standards.
- **Data Empowerment:** Give citizens control over their own data, fostering trust and enabling new data-driven business models that benefit individuals and society.
- **Intergenerational Fairness:** Ensure that the benefits of digital transformation are shared equitably across generations, avoiding the creation of new inequalities.

4. Long-Term Resilience: Critical Policy Actions

- **Prioritize Open Source:** Adopt an "Open Source First" policy for all publicly funded software projects ("Public Money, Public Code"), including **procurement** of digital solutions for the public sector in Europe. This will foster innovation, reduce vendor lock-in, enhance cybersecurity, and promote a vibrant European open-source ecosystem.
- **Enforce Interoperability:** To prevent vendor lock-in, mandate open standards for data formats, APIs, and communication protocols to ensure seamless integration and data exchange across systems and

sectors. Ensure that compliance with these standards is rigorously monitored and enforced, with clear penalties for non-compliance (for dominant players), to create a level playing field for all actors.

- **Invest in European SMEs:** Create a "European Small Business Act" that reserves a significant portion of public procurement for European SMEs and provides them with the necessary support to compete with global players.
- **Build the EuroStack:** Invest in and promote the development of a modular, scalable, interoperable, and Open Source-based digital infrastructure (the "EuroStack") built upon existing European solutions. This is a *bottom-up* approach, focused on identifying, promoting, integrating, and supporting existing European open-source technologies.
- **Strengthen Cybersecurity:** Invest in cybersecurity research and development, promote the adoption of secure coding practices, and establish clear incident response plans.
- **Develop Digital Skills:** Prioritize digital skills training, focusing on open-source technologies, cloud computing, and cybersecurity.
- **Sustainable Financing:** Implement funding models where users of EuroStack components directly contract with the entities responsible for their development and maintenance.
- **Reform or Replace Gaia-X:** The current Gaia-X initiative, due to structural flaws and the undue influence of hyperscalers, is unsalvageable. It should be either fundamentally reformed to remove conflicted interests and prioritize genuinely European, Open Source solutions, or abandoned in favor of a new initiative built from the ground up on the principles of the EuroStack.

5. Synergies and Tensions

- **Synergy:** Digital sovereignty and economic competitiveness are mutually reinforcing. A strong European digital ecosystem will create jobs, drive innovation, and enhance the EU's global competitiveness.
- **Synergy:** Open source and cybersecurity are closely linked. The transparency and auditability of open source enhance security and reduce the risk of hidden vulnerabilities.
- **Tension:** Short-term cost considerations may conflict with the long-term benefits of investing in sovereign digital solutions. However, this is a false economy; the long-term costs of dependence on non-European providers (economic vulnerability, data insecurity, lack of control) far outweigh the short-term savings.
- **Tension:** The desire for rapid deployment of new technologies may clash with the need for thorough security and ethical assessments. A balance must be struck, prioritizing security and ethical considerations without unduly stifling innovation. The use of open source and open standards facilitates this balance.

6. Enhancing Strategic Foresight

The European Commission could enhance its strategic foresight by:

- **Embracing Open Source Intelligence (OSINT):** Leveraging the vast amount of publicly available information on open-source technologies, market trends, and cybersecurity threats.
- **Engaging with the Open Source Community:** Actively engaging with the European open-source community to gather insights and expertise.
- **Developing Scenario Planning Capabilities:** Using scenario planning to explore a range of possible futures and assess the resilience of different policy options.
- **Establishing a Dedicated Foresight Unit:** Creating a dedicated unit within the Commission with the expertise and resources to conduct ongoing foresight activities.

- **Prioritizing Bottom-Up Initiatives:** Recognize and support bottom-up, community-driven initiatives like the EuroStack, which are often more agile and innovative than top-down approaches.

The EuroStack Project believes that a strong commitment to digital sovereignty, built upon Open Source principles and a thriving European ecosystem, is essential for the EU's long-term resilience. We urge the Commission to consider these recommendations in the development of the 2025 Strategic Foresight Report. We are ready to provide further input and collaborate with the Commission on this critical issue.

Sincerely,

Stefane Fermigier

On behalf of the EuroStack Project