



focis

# From Fragmentation to Federation

## Towards European Digital Resilience



eco



Funded by  
the European Union  
NextGenerationEU

Supported by:



on the basis of a decision  
by the German Bundestag

ora CLOUD-EDGE  
CONTINUUM

Version 1.0 (February, 10 2026)

ISBN: 978-3-9828074-4-7

**Published by**

eco – Association of the Internet Industry (eco – Verband der Internetwirtschaft e.V.) Lichtstrasse 43h,  
50825 Cologne, Germany

**Copyright © eco Association on behalf of FACIS - funded by the German Federal Ministry for Economic Affairs and Energy (IPCEI-CIS)**

Image Source: Adobe Stock

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA



**Commissioned author:**

**Identity Valley Research gGmbH**

Pützgasse 6, 53572 Unkel

Germany

Telefon: +49 170 407 2484

Point of contact: Jutta Juliane Meier

E-mail: [jj.meier@identityvalley.org](mailto:jj.meier@identityvalley.org)

Website: [www.identityvalley.org](http://www.identityvalley.org)

**Peer reviewed by the following people in January 2026:**

Andreas Weiss, eco – Association of the Internet Industry

## Executive Summary

Europe learned the hard way that resilience isn't about quick fixes – it's about building structures that endure. After wars that tore the continent apart, it responded by creating institutions that made cooperation the default. But that resilience was designed for an analogue world. Today, when a single software update can ground flights across a continent, and 70% of European cloud services run on non-European infrastructure, the question is no longer whether disruption will come, but whether Europe can keep essential services running when it does.

This paper argues that Europe's digital fragility does not stem from a lack of capabilities, but from how they are organised: 27 digital islands within the European Union operating in parallel, deep dependencies on a handful of external providers, and single points of failure that turn local incidents into continental crises. The CrowdStrike outage of 2024, which crashed millions of Microsoft Windows systems around the world, was a preview of this. The next disruption – whether technical, geopolitical, or hybrid – will cascade through the same vulnerabilities.

The solution isn't another centralised platform or more regulation. It's *federation*: connecting Europe's diverse systems so they work together without surrendering control to any single actor. Imagine cloud roaming like mobile roaming: services that move seamlessly across providers and borders when needed. Imagine a credible Plan B and Plan C for critical infrastructure; not on paper, but tested and ready. Imagine trust that's verifiable, not assumed.

The tools exist. The **8ra initiative**, the European umbrella effort established under the EU's IPCEI-CIS framework (Important Projects of Common European Interest – Next Generation Cloud Infrastructure and Services), offers a practical blueprint for making federation turning this vision into reality. Bringing together around 120 companies from industry, research, and technology, 8ra is building the Multi-Provider Cloud-Edge Continuum: a connected architecture enabling flexible use of distributed cloud and edge resources across providers and national borders. Projects like **FACIS** (Federation Architecture for Composed Infrastructure Services) are translating this vision into working federated cloud infrastructure; demonstrating that sovereign, interoperable alternatives are no longer theoretical, they're already under construction.

What's missing is the shift from promising pilots to shared practice, embedding resilience into procurement, standards, and market incentives so that diversity becomes a strength rather than a weakness.

The next shock will be digital. The question is whether Europe will learn from such crises – or forget them, again and again.

# Table of Contents

|  |    |
|--|----|
| Executive Summary .....  | 1  |
| 1. Introduction.....   | 1  |
| 2. Europe’s Fragmentation as a Strategic Vulnerability .....                             | 2  |
| Fragmented digital capabilities.....   | 3  |
| Critical dependencies and systemic lock-in .....   | 4  |
| Single points of failure .....   | 5  |
| 3. Strategic Vision: Empowering a Resilient, Federated, Interoperable Digital Europe ... | 7  |
| From fragmentation to federation: Building a federated digital backbone .....            | 8  |
| Achieving cloud roaming across Europe: Making digital services portable and resilient .  | 9  |
| Strengthening choice: European ‘Plan B and Plan C Readiness’ .....                       | 10 |
| Trusted Interoperability: From Control to Verifiable Trust .....                         | 11 |
| 4. From Vision to Execution: Building a Resilient European Digital Ecosystem.....        | 12 |
| Implementing the 8ra initiative at scale .....   | 13 |
| Leveraging FACIS as the federation execution engine .....                                | 14 |
| Establishing open standards and shared governance .....                                  | 15 |
| Further levers to move from vision to impact.....  | 16 |
| 5. Conclusion and What to Do Next.....   | 18 |
| References .....   | 19 |

# 1. Introduction

Europe has a long tradition of turning disruption into durable order. After wars that tore the continent apart, Europe responded by building institutions meant to stabilise society and make conflict structurally impossible, with cooperation as the default rather than a matter of political choice. That history created a particular kind of resilience. It is slower and less dramatic than the bold and rapid transformations seen elsewhere, but deeply institutional and cumulative.

However, resilience is never permanent. It must be renewed as conditions change. Today, Europe is facing another kind of stress, shaped by digital infrastructure, data, and software. The question now is not whether Europe can recover from past crises, but whether it has adapted its hard-won resilience to a world where society depends as much on physical infrastructure as on fragile, interconnected digital systems and platforms.

Cracks in Europe's resilience have been visible for some time. The COVID-19 pandemic was the first clear warning shot. It exposed how quickly modern societies struggle when critical systems come under stress, with supply chains breaking, overwhelmed hospitals, and national responses instead of coordinated action. The crisis did not create these problems; rather, it revealed long-standing weaknesses, such as data silos, fragmented infrastructure and software services, missing interoperability and redundancies, and dependencies that had been overlooked or deliberately ignored.

History shows how easily such warnings can be overlooked. In her book *Pale Rider*, for example, Laura Spinney shows how the influenza pandemic of 1918, despite its enormous human and social cost, largely vanished from collective memory, leaving societies poorly prepared for what followed. The lesson is simple: societies that fail to remember crises, and to embed their lessons in institutions and preparedness, are likely to be caught off guard again.

COVID-19 should have been a corrective moment, a chance to hard-wire those lessons into our systems and into how we run them. Whether Europe has done so remains doubtful. Are we prepared for the next crisis, whatever form it may take? And if not, what would it take to become more resilient?

In any case, the next crisis will not be analogue. Even if the trigger is biological, physical, or geopolitical, the effects will cascade through digital channels. Public services, healthcare, transport, finance, energy, logistics, communications, and emergency response all depend on digital infrastructure, cloud services, data flows, and software supply chains.

Resilience today means digital resilience – the ability to anticipate, withstand, recover from, and adapt to disruption – technologically, economically, and socially. Done well, it delivers more than protection against failure. It creates second-order benefits: competitiveness, innovation, and digital systems that genuinely serve people.

The Internet itself was originally built for resilience. Its designers assumed that components would fail and built networks that could continue functioning regardless. Europe's digital reality has drifted in the opposite direction. Capabilities are fragmented, dependencies concentrated, and critical functions increasingly sit on a small number of closed platforms.

Resilience is not a slogan. It is a design principle and a strategic governance decision. The task now is to learn from the shocks already experienced and build a shared European ability to keep society and the economy running under stress. This paper explores the obstacles and what it will take to change course.

## 2. Europe's Fragmentation as a Strategic Vulnerability

Europe has what it takes to be a global lead in the digital age. Its industries compete globally. Its research ecosystems are excellent. Its regulatory and governance models are mature. However, what is missing is a shared digital canopy – a common layer that can turn these scattered assets into collective strength, support resilience at scale, and unlock the full economic potential of the European Single Market.

Instead, the European Union operates as 27 digital islands. Whole national systems may connect, they rarely interoperate seamlessly or scale across borders.

This fragmentation undermines resilience and costs money. We are in an era of geopolitical competition, hybrid threats, and deep digital interdependence. Fragmented capabilities make it harder to coordinate responses. They also make it harder to keep critical services running and to reduce dependencies across public administrations, critical infrastructure and the private sector. At the same time, fragmentation limits Europe's ability to scale innovation and prevents the Single Market from realising its full digital potential.<sup>1</sup>

While Europe remains digitally divided, a small number of non-European providers have scaled across the continent with ease. They have embedded themselves in core digital services and public-sector operations. This imbalance deepens reliance, limits strategic choice, and increases exposure to systemic risks.<sup>2</sup>

Seen through this lens, fragmentation is not simply a technical challenge. It is a structural weakness that shapes Europe's ability innovate, protect critical services, and act strategically in the digital domain. That weakness manifests through three closely connected dynamics: **fragmented digital capabilities, critical dependencies and systemic lock-in**, and the **emergence of single points of failure**.

### Scenario – Fragmentation in practice

**Digital Islands** – In 2025, a Danish med-tech start-up spent six months negotiating and integrating separately with hospitals in Germany, Italy, and Poland, each of which had different cloud providers, national certification rules, and incompatible identity schemes. The same software had to be integrated three times, with each hospital's IT team repeating the security checks from scratch.

---

<sup>1</sup>Letta, E. (2024, April). Much more than a market: Speed, security, solidarity – Empowering the Single Market to deliver a sustainable future and prosperity for all EU citizens. European Council. <https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf>

<sup>2</sup><https://www.iss.europa.eu/publications/briefs/technical-political-when-cloud-certification-scheme-divides-europe>

## Fragmented digital capabilities

Europe's digital landscape is paradoxical. The EU has invested heavily in establishing common rules, standards, and strategic initiatives. Yet implementation and day-to-day operations remain largely national. Member states continue to design and deploy their own digital architectures, cloud strategies, certification approaches, and public-sector procurement frameworks.

### ***Fragmentation of architectures and standards***

Cloud and edge computing show this most clearly. National strategies differ widely in terms of their technological implementation, governance models, and security requirements. Certification and compliance frameworks often fail to interoperate, even when they pursue similar objectives. The prolonged and politically contentious discussions around the EU Cloud Services Cybersecurity Certification Scheme (EUCS) illustrate how divergent national positions even hinder the emergence of a genuinely common framework.<sup>3</sup>

For digital service providers operating across borders, this creates a patchwork of requirements, translating into higher costs. Cross-border service provision becomes less attractive. Digital borders reappear inside the Single Market. Many businesses report that the Single Market remains insufficiently integrated, with digital services among the most frequently cited obstacles.<sup>4</sup>

### ***Parallel systems instead of federated ones***

This fragmentation is also evident in how Europe organises its digital public infrastructure. Rather than building interoperable systems, public and private actors tend to develop parallel national systems. National clouds, government data platforms, health data spaces, and industrial data initiatives are designed for domestic use first, with cross-border compatibility treated as secondary.

This approach limits economies of scale and weakens resilience. Instead of pooling demand, redundancy, and response capacity, Europe replicates similar infrastructures multiple times. Each operates below optimal scale and follows different rules. Over time, this drives up unit costs, slows innovation cycles, and reduces competitiveness compared to large, integrated markets.<sup>5</sup>

In a crisis, disparate systems are more difficult to coordinate, harder to secure, and harder to adapt rapidly. Mutual assistance and burden-sharing across Member States become more complex precisely when cross-border cooperation is most needed. The early COVID-19 contact-tracing experience made this visible: nationally deployed apps initially lacked cross-border interoperability, limiting coordinated response until an EU interoperability gateway was introduced.

Europe's digital landscape remains dominated by parallel systems, divergent standards, and nationally bounded architectures that rarely interoperate by default. This fragmentation slows innovation and constrains Europe's ability to respond, recover, and adapt in a digitally interconnected world.<sup>6</sup>

---

<sup>3</sup>Bômont, C. (2025, November). Technical is political: When a cloud certification scheme divides Europe (Brief 2025-26). European Union Institute for Security Studies.

<sup>4</sup>The Cost of Non-Europe 2025

<sup>5</sup><https://cerre.eu/publications/competition-and-regulation-of-cloud-computing-services-economic-analysis-and-reviewbrof-eu-policies/>

<sup>6</sup>Bria, F., Timmers, P., & Gernone, F. (2025, February). EuroStack - A European alternative for digital sovereignty. Bertelsmann Stiftung.

European initiatives like Gaia-X, Manufacturing-X, and SIMPL demonstrate that federated, sovereignty-respecting alternatives to centralised cloud infrastructure are technically feasible. Gaia-X established a framework for secure cross-organisational data sharing while maintaining European regulatory compliance; Manufacturing-X applies these principles specifically to industrial supply chains; and SIMPL provides the open-source middleware to make it all work. Yet the limited real-world adoption of these projects tells its own cautionary tale: ambitious architectural visions and lengthy standardisation processes have often crowded out the fast, iterative approach needed to gain practical traction. The gap between what these federations *could* achieve and what they *have* achieved highlights just how difficult it is to compete with established platforms – not for lack of good ideas, but for lack of agile execution.

## Critical dependencies and systemic lock-in

Fragmentation within Europe has been accompanied by a second, equally consequential trend: relying more and more on non-European providers, particularly in cloud computing and core digital services. While Europe is struggling to integrate its own digital capabilities, non-European infrastructure providers have succeeded in doing exactly that.

### **Market concentration and US cloud dominance**

Currently, roughly 70% of Europe’s cloud market is controlled by non-European providers, primarily headquartered in the United States.<sup>7</sup> European providers collectively hold a significantly smaller market share, often concentrated in niche or national markets rather than operating at continental scale.

This concentration produces systemic lock-in that closely resembles the pre-roaming era in European telecommunications. Enterprises and public administrations have become dependent on specific proprietary ecosystems, APIs (application programming interfaces that define how different software systems communicate with each other), pricing models, and contractual terms. Switching providers is technically complex, operationally risky, and financially costly.

Competition authorities and regulators have repeatedly highlighted how cloud customers face high switching costs and limited interoperability, helping incumbents stay on top.<sup>8</sup> Once you’re in, you usually get pulled in deeper as additional services are layered onto the same core platforms (such as managed databases, data analytics, AI services etc.)

### **Architectural lock-in**

Lock-in is both contractual and architectural. Most European organisations have built their digital systems around centralised cloud architectures optimised for “hyperscaler” environments. These architectures prioritise efficiency and scalability under normal conditions. However, they often do so at the expense of modularity, portability, and redundancy.

Public administrations are particularly affected.<sup>9</sup> Outdated procurement practices, skills shortages, and risk-

---

<sup>7</sup>Office of Communications. (2023, October 5). Cloud services market study: Final report. Ofcom.

<sup>8</sup>Body of European Regulators for Electronic Communications. (2024, March). BEREC report on cloud and edge computing services.

<sup>9</sup>[https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/780413/ECTI\\_ATA%282025%29780413\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/780413/ECTI_ATA%282025%29780413_EN.pdf).

averse cultures have encouraged long-term reliance on single vendors, especially for critical systems.<sup>10</sup> Over time, this reliance shrinks your options and makes it harder to change course when conditions change.

The problems arising from this reliance are not hypothetical. For public-sector and sensitive workloads, the issue is not only whether systems can be migrated or diversified, but also which regulation applies or precisely which jurisdictions ultimately require access to EU data. Even when data is hosted in Europe, providers headquartered outside the EU may remain subject to non-EU legal obligations that can require disclosure.

The structural issue is that foundational digital services depend on non-European operators. That dependence weakens Europe's legally and operationally robust control over sensitive data and services. It also makes it harder to adjust quickly if conditions change. A similar uncertainty exists in the legal basis for transatlantic data transfers: EU-US arrangements have repeatedly been challenged in court, and previous frameworks have been overthrown – creating the risk that the rules can change abruptly, forcing organisations to adapt at short notice.

### **Implications for autonomy and adaptability**

Dependencies raise a fundamental issue: Europe's capacity to choose and to act. Decisions on data protection, security requirements, procurement, or industrial policy increasingly hit technical and legal limits defined outside of Europe's direct control.

From a resilience perspective, systemic lock-in reduces adaptability. Systems that cannot be reconfigured, diversified, or migrated in response to emerging risks are inherently more fragile. Dependency therefore becomes not only an economic concern but a strategic one.

## Single points of failure

The emergence of single points of failure is the most visible manifestation of the convergence of fragmentation and dependency. As Europe relies on a small number of centralised platforms, disruptions affecting these platforms can spread fast across sectors and borders. In a more contested geopolitical environment, this concentration becomes a strategic weakness. Outages affecting major cloud and digital service providers, especially those with core infrastructure services, proprietary identity systems and content delivery services, have disrupted services across multiple countries and sectors simultaneously.

### **Concentration risk and real-world disruptions**

Recent incidents have made these risks tangible. While such incidents are often framed as technical failures, their systemic impact reveals deeper structural vulnerabilities. The CrowdStrike outage in 2024<sup>11</sup> – in which a faulty software update to a widely used cybersecurity tool caused millions of Windows computers worldwide to crash simultaneously – demonstrated how a single point of failure could cascade across critical services, including transport, healthcare, and public administration.

---

<sup>10</sup>European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA). (2025, June). Sovereign cloud technologies: Is the cloud really just somebody else's computer?

<sup>11</sup>CrowdStrike: What the 2024 Outage Reveals About Security. Privacy International. (2024, December).

As global geopolitical tensions increase, there is a growing likelihood that such disruptions may be triggered or exploited, rather than occurring purely by accident. The WannaCry ransomware attack in 2017 for instance encrypted users' files and demanded payment to restore access, disrupting hospitals, businesses, and government agencies across 150 countries.<sup>12</sup> Similarly, the Mirai Botnet attacks in 2016 hijacked everyday Internet-connected devices like cameras and routers to flood key Internet infrastructure with traffic, knocking major websites offline for hours. These were early examples of how digital vulnerabilities can be weaponized at scale.

### ***Cascading effects across critical sectors***

European and international threat assessments consistently warn that cascading effects are likely to intensify. The European Union Agency for Cybersecurity (ENISA) identifies cross-border ICT service providers as a growing single point of failure in its threat landscapes and foresight reports, particularly in highly interconnected sectors such as energy, transport, and healthcare.<sup>13</sup> When core digital infrastructures are controlled externally, Europe's room for manoeuvre narrows – both in day-to-day operations and in moments of political or security stress.

Healthcare offers a vivid illustration of this. ENISA's health sector threat landscape shows how cyber incidents affecting shared digital services can disrupt patient care, delay treatments, and endanger the safety of entire health systems. Similar vulnerabilities exist in manufacturing, logistics, and public services, where digital downtime translates rapidly into physical and economic harm.

### ***Hybrid threats and geopolitical exposure***

Single points of failure also make Europe more vulnerable to pressure and disrupt. State and non-state actors are increasingly combining cyber operations, supply-chain manipulation, disinformation, and legal pressure to exploit systemic weaknesses.<sup>14</sup> Dependence on foreign-controlled infrastructures creates opportunities for coercion, surveillance, or disruption, particularly in periods of geopolitical tension.

At the core of these vulnerabilities lies a simple problem: a lack of redundancy. Highly centralised systems may be efficient, but they are not resilient by default. Without federated alternatives, interoperable architectures, and the ability to shift workloads across providers and jurisdictions, failures inevitably cascade. This runs counter to the original logic of the Internet itself: it was designed as a distributed network that could keep functioning even when individual nodes failed, precisely to avoid catastrophic single points of failure.

Resilience, as increasingly recognised in EU critical infrastructure policy, depends on diversity, decentralisation, and the capacity to absorb shocks without systemic collapse. Europe's current digital configuration falls short on all three counts.

---

<sup>12</sup><https://www.wired.com/2017/05/wannacry-ransomware-ddos-attack/>

<sup>13</sup>ENISA Foresight 2030 Threats Report. European Union Agency for Cybersecurity. (2023, March). Identifying emerging cyber security threats and challenges for 2030.

<sup>14</sup>Nelson, J., & Sánchez, I. (2025, May). Alone we stand: How Europe can counter hybrid threats in a post-transatlantic era. European Council on Foreign Relations.

### Scenario – Concentration risk in practice

**When the hyperscaler blinks** – In 2026, most European payment and ticketing services still depend on a handful of global cloud regions and providers. A major outage in one region means that trams in a central European capital stop accepting card payments, small shops can't process transactions, and online public services slow to a crawl. Citizens are told to "try again later".

## 3. Strategic Vision: Empowering a Resilient, Federated, Interoperable Digital Europe

Europe's digital fragility does not stem from a lack of capability, but from the way its capabilities are organised. They are too fragmented across borders, dependent on a narrow set of external providers, and increasingly concentrated in single points of failure. In such a setting, ad-hoc solutions won't deliver resilience. It has to be designed into the system itself; embedded in the architectures, governance models, and market structures that shape how digital services are built and connected.

Digital resilience, in this sense, is the **ability to anticipate, withstand, recover from, and adapt to disruption** – across technological, economic, institutional, and social dimensions. European threat assessments and policy frameworks are increasingly reflecting this understanding. Crucially, resilience goes beyond cybersecurity or critical infrastructure protection. It encompasses the continuity of (public) services, the integrity of communication and markets, and the preservation of trust in digital systems.<sup>15</sup>

Therefore, resilience should not be understood as merely defensive capacity. It is not just about surviving attacks or bouncing back from failures. When resilience is built into the design of digital systems from the start, good things happen:

- You avoid single points of failure, which lowers systemic risk;
- You reduce switching costs, which increases competition;
- You enable modularity and recombination, which supports innovation and competitiveness.

Europe's strategic challenge is not to add resilience to existing architectures as an afterthought. The task is to re-architect our digital ecosystem so that resilience becomes intrinsic. That requires a fundamental shift in perspective from centralisation to federation. This way, Europe's diversity, so often seen as a weakness, will become a cornerstone of its resilience.

---

<sup>15</sup>See, i.a.: Directive (EU) 2022/2555 (NIS2), which links cybersecurity requirements to the security and continuity of essential services; Directive (EU) 2022/2557 (CER), which targets the resilience and continuity of critical entities and vital societal functions; and the EU Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final) together with the EU Cybersecurity Act (Regulation (EU) 2019/881), which emphasise trustworthy digital technologies and EU-wide certification to support trust in digital systems.

## From fragmentation to federation: Building a federated digital backbone

Europe's digital landscape remains fragmented. National and sectoral systems have developed in parallel rather than as parts of a coherent whole. However, this fragmentation is not the result of missing capabilities. Europe already has a dense and sophisticated digital base: national cloud initiatives, sector-specific data platforms, industrial edge infrastructures, and advanced public digital services. The strategic weakness lies in the absence of federation by design.

A federated digital backbone gives Europe a way out. Each participant, whether a public authority, an infrastructure provider, or an industrial platform, retains control over its own systems and data while gaining the ability to interoperate seamlessly with others. Federation does not mean replacing existing systems with a single European platform. It connects heterogeneous systems through shared design rules, interoperable interfaces, and common governance rules.

This approach addresses the limitations of the two extremes that Europe has oscillated between. Purely national solutions lack scale and resilience. Highly centralised models concentrate risk and create dependency. Federation offers a third path: distributed integration, where resilience emerges from diversity rather than homogeneity.<sup>16</sup>

Think about what this means in practice. Workloads, data, and services would no longer be statically bound to one provider or location. They could move dynamically across providers and borders based on operational, regulatory, or resilience requirements. Europe's risk would drop sharply. A localised failure – be it technical, legal, or geopolitical – would not automatically cascade into systemic disruption, because alternatives would be available.

The strategic implications extend beyond infrastructure resilience. Federation is also a prerequisite for a functioning Digital Single Market in practice. Persistent fragmentation has hindered European digital providers from scaling beyond national markets, promoting dependency on a small number of non-European providers.<sup>17</sup> By reducing technical and contractual barriers to cross-border service provision, federation enables European providers to compete on quality, specialisation, and trust rather than sheer size.

Federation transforms Europe's diversity from a constraint into a competitive advantage. Different providers can specialise in different domains (security, performance, sectoral compliance) while remaining interoperable within a shared ecosystem. The result is a plural yet coherent digital market, capable of supporting innovation while maintaining resilience.

---

<sup>16</sup>Bria, F., Timmers, P., & Gernone, F. (2025, February). EuroStack - A European alternative for digital sovereignty. Bertelsmann Stiftung. <https://www.bertelsmann-stiftung.de/en/our-projects/reframetech-algorithmen-fuers-gemeinwohl/project-news/eurostack-a-european-alternative-for-digital-sovereignty>

<sup>17</sup>Bomont, C. (2025, November). Technical is political: When a cloud certification scheme divides Europe (Brief 2025-26). European Union Institute for Security Studies. <https://www.iss.europa.eu/publications/briefs/technical-political-when-cloud-certification-scheme-divides-europe>

**Scenario – Federation in practice**

**A small city without a big IT department** – A mid-sized city in eastern Europe wants to modernise its services: online building permits, kindergarten registration, local tax payments. In 2026, it has two options; both bad: lock itself into a contract with one large vendor, or try to stitch together national systems and local providers on its own. Either way, the city's tiny IT team is overwhelmed. With a federated backbone in place, the city can choose from a set of ready-made building blocks already used by other municipalities in Europe. Identity, payments, archiving and hosting come from different providers – some public, some private, some cross-border – but they are designed to work together. The city can swap out a provider that becomes too expensive or untrustworthy, without rebuilding everything from scratch.

## Achieving cloud roaming across Europe: Making digital services portable and resilient

One of the most tangible benefits of a federated digital backbone is "cloud roaming". It keeps services available and makes it possible to move them across Europe when needed, regardless of their location or the hosting provider.

The analogy with mobile telecommunications is useful here. Before roaming, crossing a border often meant losing connectivity, swapping SIM cards, or accepting a degraded service. Roaming changed all that by aligning technical standards, building trust between operators, and harmonising regulatory expectations. Users stayed connected while providers still competed.

Europe's cloud landscape today resembles that pre-roaming era. Services are tightly bound to specific platforms, contracts, and jurisdictions. Moving workloads for cost, resilience, compliance, or geopolitical reasons is still slow, risky, and hard.

Cloud roaming reverses this. In a roaming-enabled environment, services and workloads can move between providers and across borders without breaking security, compliance, or service guarantees. This reduces systemic risk because a disruption at one provider does not need to cascade across sectors. This vision aligns directly with what 8ra aims to achieve: a connected network of European cloud and edge capacity that supports seamless transitions without compromising governance or service levels.

This requires more than just technical portability. It depends on trust at scale. Providers must be able to rely on each other's assurances on identity, security posture, compliance status, and service quality. If that trust layer is in place, Europe can rely less on complex redundancy inside single platforms and more on diversity across providers and jurisdictions. Workloads can be redeployed during outages. Services can be relocated when regulatory or geopolitical conditions change.

Cloud roaming also has economic benefits. By lowering switching costs and reducing lock in, it increases competitive pressure and encourages innovation. Providers compete on quality, trust, and specialisation rather than on trapping customers in proprietary ecosystems.

Such a cloud mesh does not require uniformity. Different providers can keep different infrastructures, business models, and sectoral specialisations. What matters is a shared infrastructure management layer that makes them interoperable and keeps the market from fragmenting.

## Strengthening choice: European 'Plan B and Plan C Readiness'

A stronger European digital position is one in which governments, businesses, and citizens are never structurally tied to a single provider or platform without credible alternatives, a practical Plan B and Plan C that can be activated when conditions change.

Many European public administrations and enterprises are deeply embedded in centralised cloud and software ecosystems optimised for specific providers. Even when alternatives exist in principle, switching is often perceived as too costly, risky, or disruptive to be a realistic option.

Federation directly addresses this problem. When services are designed to be interoperable across providers and borders, switching becomes a realistic option. Federation keeps Plan B and Plan C viable, even if they are not used every day. The goal is not constant movement, but the credible ability to switch when needed.

Public authorities play a pivotal role in restoring this capacity for choice. The government primarily acts as a **regulator and guarantor of resilience**, establishing strict security standards and legal frameworks that compel operators to protect critical digital infrastructure from cyber threats and failure. Simultaneously, public authorities usually act as the **central coordinator for crisis management**, monitoring systemic risks and facilitating a rapid response to ensure the continuity of essential services such as energy, water, and transport.

As major buyers of digital services and custodians of critical functions, public administrations can shape market behaviour through procurement, funding, and programme design. By requiring interoperability, portability, and federation-readiness in public tenders and initiatives, they create demand-side incentives that shift the market toward openness and substitutability.

This approach is not about excluding non-European providers. Federation and roaming are neutral with respect to provider origin. What they require is adherence to shared rules on interoperability, security, and trust.

At a systemic level, 'Plan B and Plan C readiness' aligns directly with resilience. Systems with credible alternatives can adapt under stress. Systems without alternatives become brittle. Federation helps ensure Europe's digital ecosystem remains adaptable in the face of uncertainty, volatility, and strategic competition.

## Trusted Interoperability: From Control to Verifiable Trust

Federation is often discussed in infrastructural or architectural terms. However, its purpose is operational and strategic. It enables organisations to collaborate, scale, and innovate across boundaries without being locked into isolated or vertically integrated environments. A resilient European digital ecosystem, therefore, depends on interoperability that supports cooperation without increasing dependency or risk.

Historically, interoperability efforts have focused on technical interfaces – data formats, APIs, and protocols. These elements are necessary but not sufficient. Effective interoperability in a federated environment also depends on trust in rules, contracts, and day-to-day operations. Without trust, technical connectivity can amplify exposure and liability rather than enabling sustainable collaboration.

In Europe's diverse legal, regulatory, and market landscape, trust cannot rely solely on central control or uniform governance structures. Instead, it must be verifiable and context-aware. This requires a shift from control-based interoperability where access is granted through static permissions and central authorities to trust-based interoperability, where access is automatically granted based on verified attributes, shared rules, and clearly defined purposes.

European identity and trust frameworks provide the basis for this shift. Initiatives such as eIDAS (Electronic Identification, Authentication and Trust Services) and EUDI (European Digital Identity Wallet) aim to make digital identity seamless, secure, and user-controlled across Europe, allowing people to easily share verified credentials such as a driver's license or diploma. More recently, the European Business Wallet<sup>18</sup> has extended that approach to organisations, enabling businesses to prove their legitimacy and conduct cross-border transactions with less administrative burden. Together, these initiatives aim to ensure that attributes can be recognised across borders and across sectors. They matter because they enable systems work together securely and faster. In practice, organisations (and individuals) need to prove specific attributes, such as certification status, regulatory compliance, or contractual role, without disclosing unnecessary information or surrendering control over their assets.

This approach enables access to data and services only when needed. Resources can be shared precisely where, when, and with whom they are required, based on predefined policies and business purposes. Access becomes granular, auditable, and revocable rather than binary or permanent. This is particularly critical in regulated sectors such as healthcare, aviation, energy, and public administration. In these settings, cross-organisational cooperation must coexist with stringent compliance and accountability requirements.

From an ecosystem perspective, trusted interoperability strengthens both resilience and competitiveness. It reduces integration costs, limits systemic risk, and increases flexibility in partner selection. It also supports continuity of operations under stress, enabling organisations to adapt and reconfigure supply chains, service networks, and data flows without relying on single points of control.

---

<sup>18</sup> <https://digital-strategy.ec.europa.eu/en/policies/business-wallets>

**Scenario – Trusted interoperability in practice**

**The cross-border patient** – A woman living near the Czech-German border has a chronic condition and regularly sees doctors on both sides of the border. In 2026, every visit begins with the same paper forms, repeated explanations, and often a USB stick or CD with past scans. Each hospital's system treats her as a new case. In a human-centric interoperable setup, she uses a European Digital Identity Wallet to share a minimal set of verified health data with both care teams. Consent, language and data-protection rules are built into the process. Her German specialist sees that a Czech hospital has already performed certain tests and can build on that information instead of repeating it. For her, "European interoperability" is not an abstract policy – it means fewer repeats, fewer errors, and better care with less costs.

## 4. From Vision to Execution: Building a Resilient European Digital Ecosystem

The strategic direction is clear. Europe must build a federated digital backbone, facilitate real portability across providers and borders, develop credible alternatives for critical services, and ensure interoperability based on verifiable trust.

However, vision alone does not create resilience. The difference between ambition and impact lies in execution. Over the past decade, the EU has set out strategies on cloud computing, data spaces, cybersecurity, and digital sovereignty. Yet implementation has often remained uneven or confined to pilots. Too many initiatives show what is possible without establishing it as common practice.

If federation, cloud roaming, and digital resilience are to become defining features of Europe's digital ecosystem, they must be built into the system itself and continuously maintained. That means shared reference architectures, trust mechanisms that work in day-to-day operations, and investment and procurement practices that are aligned.

The following section highlights where Europe is already on the right track and what it still needs to make a federated model work at continental scale. 8ra and FACIS are presented as leading examples. Further recommendations are added to close the gap between vision and impact.

## Implementing the 8ra initiative at scale

The 8ra initiative is one of Europe's most comprehensive attempts to make a federated, resilient digital ecosystem a reality.<sup>19</sup> Conceived as a cloud–edge continuum spanning multiple providers, sectors, and EU Member States, it aims to provide a shared foundation through which Europe's fragmented capabilities can work together at scale. It speaks directly to the challenges identified earlier: fragmentation, dependency, and concentration risk.

8ra's strategic contribution is not a single platform. It is a shared approach that helps different systems connect in predictable ways, without removing national or sectoral control. Done well, it makes it easier to move services when needed and cuts reliance on a single provider.

### ***From pilots to a shared fabric***

At present, 8ra consists of projects, pilots, and use cases. This phase is valuable because it builds expertise and shows demonstrates feasibility. However, to matter structurally, 8ra needs to become a shared fabric rather than a set of separate implementations. That shift depends on reference architectures. These are practical blueprints that describe how federation should work across the cloud-edge continuum, including how organisations join, how trust is established, how policies are applied, how services are combined, and how portability and failover should function. They do not impose uniformity. They reduce the risk of each project building its own version of federation, which would recreate fragmentation and keep cross-border cooperation costly.

Scaling also requires alignment across Member States, public authorities, and industry. This alignment is practical. It involves agreeing on a small set of federation expectations and linking them to funding and procurement. If procurement keeps rewarding tight coupling to one supplier, portability will stay theoretical, and alternatives will remain weak.

Implementing 8ra at scale requires a clear link between architectural decisions and resilience outcomes. As pointed out before, federation is not an end in itself, but rather a means of reducing single points of failure, mitigating dependency, and enabling continuity of services under stress.

This means resilience criteria (e.g. redundancy across providers, failover capabilities, jurisdictional diversity) should be explicitly incorporated into federation governance and evaluation frameworks. Architectural decisions must contribute directly to Europe's strategic resilience, not merely increase technical sophistication.

In this sense, 8ra can be understood not only as an infrastructure initiative, but as a resilience instrument. Above all, its implementation may determine whether Europe can translate strategic intent into operational robustness.

---

<sup>19</sup> <https://www.8ra.com/>

## Leveraging FACIS as the federation execution engine

While 8ra provides direction and a frame, FACIS (Federation Architecture for Composed Infrastructure Services) provides the tools that make federation practical to implement.<sup>20</sup> Its value lies in reducing the bespoke integration work that repeatedly blocks cross-border scaling.

FACIS does this through Federation Architecture Patterns (FAPs). A FAP is a reusable blueprint for how services can be combined across providers, sectors, and jurisdictions. Imagine a self-driving car travelling from Budapest to Madrid. As it crosses each border, it must seamlessly switch between different cloud-edge providers while maintaining the same service quality. FAPs provide the blueprints for these automatic handovers. In other words, they allow cross-border, multi-provider services to be built in a repeatable way, defining who plays which role, what information needs to be exchanged, and what level of trust is required. They transform the concept of federation from a concept into a consistent approach for building and running services across providers and borders.

### ***Trust that works across providers***

Federation increases connectivity. However, without strong trust mechanisms in place, connectivity alone can also increase exposure. FACIS addresses this issue by embedding trust into the patterns so that onboarding and access decisions rely on verifiable attributes, not informal assurances. This way, organisations can (and need to) prove what matters, such as certification, compliance status, or contractual role, in ways that are context-specific, auditable and revocable. This reduces friction while keeping accountability clear, especially in heavily regulated environments.

This trust layer is also what makes portability workable. Moving a service between providers is not only a technical migration. It is a handover of responsibilities, assurances, and rights. Without a shared method of verifying trust and permissions among participants, portability remains slow, risky, and case-by-case.

### **Scenario – FACIS in practice**

**One click instead of three lawyers** – A Portuguese software SME has built a simple app that helps citizens track their home’s solar energy production. Three municipal utilities – one in Portugal, one in Slovenia, and one in Belgium – want to pilot the app. In 2026, each utility sends its own contract template, in a different language, with different rules for data use and liability. Instead of improving the product, the SME’s founder spends weeks going back and forth with lawyers.

In the FACIS world, however, the utilities and the SME use a shared “digital handshake” service. The founder logs in with a verified company identity, selects a standard contract template for this type of service, and agrees to the same basic terms with all three utilities simultaneously. Details like price and duration can still be negotiated – but the structure, legal language and technical conditions are standardised. Cross-border business starts to feel manageable for a small company.

---

<sup>20</sup> <https://www.facis.eu/>

### **The mechanics of portability**

Portability only works if responsibilities move with the service. When several providers are involved, you need continuity of obligations and clear accountability. FACIS does this with three building blocks: machine-readable service commitments (Service Level Agreements or SLAs), a governance layer that clarifies who is responsible for what, and a digital contracting service.

Think of it like rail travel across borders. It is not enough that the tracks connect. You also need a shared timetable, clear rules about who fixes what when something breaks, and tickets that are recognised everywhere.

Machine-readable SLAs are the timetable. They convert promises on availability, performance, and response times into terms that can be checked automatically. That makes it easier to spot problems early and to track service quality across provider boundaries.

The SLA Governance Framework is the rulebook for handling disruptions. It keeps roles clear during incidents, so responsibility does not get lost between providers.

The Digital Contracting Service is the ticketing system. It reduces legal and administrative friction by supporting verifiable digital agreements, so a service can switch providers or move workloads without renegotiating the whole contract each time.

### ***Scaling beyond pilots***

FACIS will only have a structural impact if its patterns and components become part of Europe's default toolkit, rather than remaining a set of isolated demonstrations. That means embedding FAPs, machine-readable SLAs, SLA governance, and digital contracting into reference architectures such as 8ra, into sectoral initiatives, and into procurement requirements. Once these elements are being used routinely, portability stops being a special project and becomes a normal operational option. That is what keeps Plan B and Plan C credible when conditions change.

## **Establishing open standards and shared governance**

8ra can help to coordinate a federated cloud-edge continuum across many providers, sectors, and Member States. FACIS complements this with practical building blocks for real deployments. For both to deliver lasting resilience, Europe also needs institutional "mortar" to make federation work in everyday operations. This involves shared open standards, shared governance, and practical ways to show trust and accountability across borders and providers.

Open standards are essential for portability, competition, and resilience. They enable users to switch providers, reroute data, and add new services without getting trapped in proprietary ecosystems. In a federated environment, standards are what make diversity workable. Without them, interoperability becomes costly one-off integration.

Europe already has important elements in this landscape. Initiatives such as Gaia-X, NIS 2 – the EU directive establishing cybersecurity requirements for critical infrastructure operators – and EU cloud certification

schemes contribute building blocks around trust, security, and assurance.<sup>21</sup> Their impact, however, depends on consistent interpretation and use across Member States and sectors. Applied unevenly, they can produce new silos under new labels.

The priority should be focus, not creating more frameworks. Europe should concentrate on a limited set of standards and profiles that directly support federation. These should cover technical interfaces, identity and trust, security assurance, and service quality measures that can be checked. This is what makes portability and cross-border operations manageable at scale.

Standards alone are not enough. Federation also requires shared governance. Too much central control stifles innovation, while too little coordination sustains fragmentation. The goal is to find a workable middle ground: multi-stakeholder governance with clear rules and mutual trust. The European Union establishes common principles and legal frameworks that either apply directly in the individual Member States or require national implementation.

Industry and civil society provide operational expertise. The idea is to align expectations across borders so that cooperation does not depend on constant negotiation.

Bra and FACIS can anchor this in practice. Reference architectures and patterns should spell out roles, interfaces, and trust requirements. This makes governance less dependent on manual oversight and political bargaining. Rules emerge in how systems are built and run, which makes cooperation more predictable.

Accountability is especially important when services are composed from components run by different providers. Mechanisms such as machine-readable SLAs, verifiable credentials, and auditable trust processes can help. They make it possible to check obligations and compliance continuously, and to show who is responsible for what across provider boundaries.

Done well, standards and governance become enablers. They support innovation while protecting security, rights, and resilience. They also help federation scale. This reduces the risk of drifting back into fragmentation or towards over-centralisation.

## Further levers to move from vision to impact

Beyond architectures and patterns, Europe needs levers that change behaviour at scale. The point is to make resilience a requirement that is bought, measured, and exercised, not just designed.

One such lever is public procurement. The European Commission's announced Public Procurement Act for 2026 creates a timely opportunity to hard-wire resilience into public tenders, especially for critical systems. Public buyers should require 'Plan B and Plan C readiness' as a baseline. That means portability and exit plans. It also means tested failover, clear dependency mapping, and federation-ready interfaces. Once these become standard tender conditions, resilience stops being optional 'best practice' and becomes a market expectation.

---

<sup>21</sup> European Digital SME Alliance. (2024, September). EUCS - An opportunity for Europe's digital sovereignty [Policy paper]. <https://www.digitalsme.eu/changes-to-the-eu-cloud-services-cybersecurity-certification-scheme-put-eu-citizens-data-at-risk-a-call-for-digital-sovereignty/>

Procurement becomes a stronger resilience lever when progress can be assessed and compared. Public authorities and regulators should agree on a small set of practical resilience indicators that can be used in tenders and oversight. Examples include time-to-switch for critical workloads, the concentration of key dependencies, whether failover has been tested, and verified use of federation profiles. These indicators should then be linked to incentives, such as scoring advantages, framework eligibility, or preferred supplier status for providers that can demonstrate tested continuity and portability.

One practical way to accelerate implementation is to invest in reusable building blocks that administrations can adopt without having to start from scratch. The Digital Commons EDIC (European Digital Infrastructure Consortium), launched in December 2025, is designed to do exactly this by pooling Member State resources around open, interoperable “digital commons” and helping move from isolated pilots to shared, scalable infrastructure<sup>22</sup>. Public procurement and funding programmes should actively route demand through such shared components, to build resilience once and reuse it many times across Europe.

A second lever is reducing cross-border friction for trust and contracting. The Commission’s proposed regulation on European Business Wallets can be used to make onboarding into federated ecosystems faster and more reliable. Already now, public and private operators should plan to use business wallets. These can support verified organisational identity, credentials, and authorised roles. This reduces reliance on manual checks, repeated paperwork, and slow bilateral processes in cross-border collaboration.

A third lever is the physical capacity that federation depends on. A federated cloud–edge ecosystem makes little sense without enough distributed, high-assurance compute and data centre capacity in Europe to host critical workloads with geographic diversity. The planned Cloud and AI Development Act should, therefore, be used not only to expand capacity and streamline deployment, but also use that capacity to improve resilience: more geographic spread, clear security assurance, and compatibility with federated approaches rather than new forms of lock-in. In short, the ‘hardware side’ of federation requires the same attention as the software and governance aspects.

### Scenario – Digital responsibility in practice

**The human layer of digital resilience** – A city procurement team wants to introduce a messaging and scheduling app for staff. There are two tools that can do the job. One has vague data practices and confusing default settings. The other is clear about what data it collects, offers privacy by default, and makes data export easy. The city chooses the clearer option and turns those requirements into its next tender. Digital resilience is not only built through infrastructure and regulation. It also depends on everyday choices by citizens, employees, and organisations. Over time, those choices shape which services thrive. To make these choices repeatable, people need simple guidance. Frameworks such as the Digital Responsibility Goals (DRGs)<sup>23</sup> translate the concept of ‘trustworthy digital services’ into practical objectives, covering areas such as cybersecurity, privacy, transparency, and human agency.

<sup>22</sup> European Commission. (2025, December). *Digital Commons EDIC launches to advance Europe’s technological sovereignty*. Shaping Europe’s Digital Future. <https://digital-strategy.ec.europa.eu/en/news/digital-commons-edic-launches-advance-europes-technological-sovereignty>

<sup>23</sup> <https://identityvalley.eu/digital-responsibility-goals>

## 5. Conclusion and What to Do Next

Europe's digital resilience challenge is no longer about recognising the risks. It is about building the capacity to keep essential services running when conditions change, and to adapt without being trapped by single points of failure or hard dependencies. Federation, cloud roaming, and trusted interoperability offer a viable path, but only if they evolve from promising initiatives into shared practice.

The next steps are straightforward:

- Make federation a reality in critical systems. Scale 8ra through common reference architectures and measurable resilience outcomes. Embed FACIS patterns and tools where multi-provider, cross-border services are needed most.
- Lay the institutional mortar. Agree on a small set of open standards and profiles and put shared governance and accountability mechanisms in place so cooperation works day to day, not just in pilots.
- Use incentives to shift the market. Update procurement so 'Plan B and Plan C readiness' becomes a default requirement. Agree on a short list of resilience indicators that can be checked and compared. Reward providers that demonstrate tested continuity and portability.
- Ensure the capacity exists. Treat computing and data centre capacity as part of resilience policy so federation has real options in practice, not only on paper.
- Keep the coalition alive. Meet regularly, for example at the European Resilience Summit (ERS), to maintain a shared agenda, run cross-border exercises, and turn lessons into updates to standards, procurement templates, and reference architectures. Reach out to wider industrial-policy and investment efforts so execution and adoption reinforce each other.

The goal is not to create a single European platform. The goal is digital resilience in the full sense of the term. Europe should be able to anticipate disruption, withstand it, recover, and adapt, while keeping essential services running and trust intact. The task now is to embed these lessons in our systems, markets, and institutions, so that the next shock does not catch us off guard – again.

## References

- 8ra. (n.d.). *The European multi-provider cloud-edge continuum*. <https://www.8ra.com/>
- Body of European Regulators for Electronic Communications. (2024, March). *BEREC report on cloud and edge computing services*. BEREC.
- Bômont, C. (2025, November). Technical is political: When a cloud certification scheme divides Europe (Brief 2025-26). European Union Institute for Security Studies. <https://www.iss.europa.eu/publications/briefs/technical-political-when-cloud-certification-scheme-divides-europe>
- Bria, F., Timmers, P., & Gernone, F. (2025, February). *EuroStack – A European alternative for digital sovereignty*. Bertelsmann Stiftung. <https://www.bertelsmann-stiftung.de/en/our-projects/reframetech-algorithmen-fuers-gemeinwohl/project-news/eurostack-a-european-alternative-for-digital-sovereignty>
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*, L 333, 80–152.
- Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive). *Official Journal of the European Union*, L 333, 164–198.
- European Commission. (2020). *The EU's Cybersecurity Strategy for the Digital Decade* (JOIN(2020) 18 final).
- European Commission. (2025, December). *Digital Commons EDIC launches to advance Europe's technological sovereignty*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/news/digital-commons-edic-launches-advance-europes-technological-sovereignty>
- European Commission. (n.d.). *European Business Wallets*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/business-wallets>
- European Digital SME Alliance. (2024, September). *EUCS – An opportunity for Europe's digital sovereignty* [Policy paper]. <https://www.digitalsme.eu/changes-to-the-eu-cloud-services-cybersecurity-certification-scheme-put-eu-citizens-data-at-risk-a-call-for-digital-sovereignty/>
- European Parliamentary Research Service. (2025). *The cost of non-Europe 2025*. European Parliament.
- European Union Agency for Cybersecurity. (2023, March). *ENISA foresight 2030 threats report: Identifying emerging cyber security threats and challenges for 2030*. ENISA.
- European Union Agency for the Operational Management of Large-Scale IT Systems. (2025, June). *Sovereign cloud technologies: Is the cloud really just somebody else's computer?* eu-LISA.
- FACIS. (n.d.). *Federation Architecture for Composed Infrastructure Services*. <https://www.facis.eu/>
- Gineikyte-Kanclere, V., et al. (2025). *European software and cyber dependencies* (Publication for the Committee on Industry, Research and Energy). Policy Department for Transformation, Innovation and Health, European Parliament. [https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/780413/ECTI\\_ATA\(2025\)780413\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/780413/ECTI_ATA(2025)780413_EN.pdf)
- Identity Valley. (n.d.). *Digital Responsibility Goals*. <https://identityvalley.eu/digital-responsibility-goals>
- Letta, E. (2024, April). *Much more than a market: Speed, security, solidarity – Empowering the Single Market to deliver a sustainable future and prosperity for all EU citizens*. European Council. <https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf>
- Manganelli, A., & Schnurr, D. (2024, February). *Competition and regulation of cloud computing services: Economic analysis and review of EU policies*. Centre on Regulation in Europe (CERRE). <https://cerre.eu/publications/competition-and-regulation->

[of-cloud-computing-services-economic-analysis-and-reviewbrof-eu-policies/](#)

Nelson, J., & Sánchez, I. (2025, May). *Alone we stand: How Europe can counter hybrid threats in a post-transatlantic era*. European Council on Foreign Relations.

Office of Communications. (2023, October 5). *Cloud services market study: Final report*. Ofcom.

Privacy International. (2024, December). CrowdStrike: What the 2024 outage reveals about security. *Privacy International*.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification (EU Cybersecurity Act). *Official Journal of the European Union*, L 151, 15–69.

Spinney, L. (2017). *Pale rider: The Spanish flu of 1918 and how it changed the world*. Jonathan Cape.

Wired. (2017, May). The WannaCry ransomware attack. *Wired*. <https://www.wired.com/2017/05/wannacry-ransomware-ddos-attack/>