Disclaimer: This paper does not aim to address issues related to defence and national security whose particular characteristics call for a specific, tailored framework. Pursuant to Article 4(2)(3) of the EU Treaty, these areas fall within the sole responsibility of the Member States.

Note: The present paper is of a political nature and sets out the key points of the common understanding of France and Germany of digital sovereignty. As such, it seeks to provide impetus to and guidance on the upcoming discussions and legislative work at EU level.

Franco-German Joint Paper on Digital Sovereignty

1 General goal

Urgency

Europe's digital sovereignty needs to be strengthened by reducing critical dependencies on digital technologies, resources, products and services from third countries. Critical dependencies exist across the entire technology stack, from IT infrastructure (incl. semiconductors) and software to data handling and artificial intelligence and across all sectors.

Each Member State's digital sovereignty is inextricably linked to Europe's digital sovereignty. While national measures are essential, securing digital sovereignty comprehensively and sustainably requires European coordination and cooperation around clear goals. Europe aims for a digital transformation based on shared values, standards and interests, enabling it to position itself as an independent actor in the global economy and geopolitical competition.

Recent geopolitical upheavals and increasing systemic competition make it a strategic imperative to ensure areas of Europe's strategic influence, reduce strategic dependencies and vulnerabilities and avoid lock-in effects. Globally, digital technologies are now at the core of economic value chains and competitiveness. The Draghi report shows a clear link between digital sovereignty and macroeconomic stability. Digital sovereignty is therefore essential for economic security.

Given the geopolitical situation, digital sovereignty is more than ever also a crucial security challenge. Cyberattacks, security breaches, cyber espionage and hybrid threats increasingly target digital infrastructures as nervous systems of our democracies, economies and societies. Supply chain disruptions, for example for chips, can take place anywhere in the manufacturing process. They could lead to production stoppages at certain key suppliers and threaten availability of the necessary hardware. At the same time, open markets and international cooperation with trusted partners remain essential pillars of European digital sovereignty.

Furthermore, strengthening digital sovereignty also entails creating the conditions necessary to effectively conduct criminal investigations and legal proceedings against cybercriminals, state-sponsored attackers, and other actors who threaten digital infrastructure. Therefore, strengthening the EU's digital sovereignty ensures that European value creation and security go hand in hand.

Increasing the EU's digital sovereignty does not mean turning towards protectionism and isolationism, thus, EU Member States intend to continue to cooperate with trusted international partners. This means, in particular, partners that respect human rights, democratic principles and the rule of law as well as meet fundamental standards for the protection of data. Moreover, international legal obligations from bilateral or multilateral treaties and free trade agreements will need to be respected and fulfilled.

Within the framework of collective security systems, the highest priority should lie on joint action capability in order to guarantee alliance capability for collective deterrence and defence. Against the background of Article4(2)(3) of the EU Treaty, this paper explicitly does not aim to address issues related to defence and national security.

In addition, this paper does by no means aim to impose any conditions on any private-sector companies regarding private procurement but it can constitute a toolbox for the assessment of their dependencies and monitor their procurement.

Finally, this paper does neither create any obligation of an EU Member State to make investments nor otherwise entail any additional expenditures from public budget. If the criteria laid down in this document should be applied in the context of public expenditure, this will be subject to funding approval in accordance with the relevant principles of budgetary law, with the allocation of budgetary funds taking place as part of the relevant budget formulation process. The principles of proportionality and cost efficiency are applicable.

Aspiration

Europe needs to strengthen its own digital ecosystem. This ecosystem will build on a foundation of both EU-wide initiatives and nationally-driven innovation, respecting the principle of subsidiarity to ensure the most effective allocation of resources and responsibilities. Digital technology is at the heart of almost all value chains and thus of economic growth, and dependencies expose economies to systemic vulnerabilities that weaken European sovereign decision making in the long term.

In Europe, most digital companies have fewer than 250 employees.[1] They innovate, but face challenges in scaling up. Without targeted action, Europe risks remaining a continent of innovation with too few economic players of global scale. Europe’s approach reflects its ambition to strengthen its role as a producer, standard-setter, and strategic shaper of technological development.

This paper provides a shared framework for strengthening Europe's capacity to act in the digital domain, combining resilience, competitiveness and technological capability. This includes both defensive and proactive approaches: defensive refers to the protection against external coercion (whether through legal means or technological restrictions), safeguarding of strategic assets, and protection of sensitive data. The proactive approach, on the other hand, refers to the independent decision-making capacity by supporting educational, research, innovation and economic security objectives and strengthening European digital value chains in supporting development, deployment and use of digital infrastructure, technologies and services. This joint paper seeks to support a coherent and operational European response across policy fields.

It also aims to nourish the European Commission’s current reflections on the various legislative vehicles under discussion in 2026 (Tech Sovereignty Package, including the Cloud and AI Development Act) and beyond, while providing a longer-term vision of European digital sovereignty for the next years.

As this paper aims at defining the dimensions and criteria of digital sovereignty and trying to make this concept as operational as possible, it could also be a voluntary reference framework for the ecosystem to assess the vulnerabilities of the digital aspects of its activity.

[1] European Commission / JRC, *Annual Report on European SMEs 2024/2025*, Table 17 (“Industrial Ecosystems: Proportion of Economic Activity by Size Class (2024)”), line “Digital”.

Definition

Digital sovereignty is the capability and capacity to develop, provide, use, adapt and control digital technologies including hardware in an independent, self-determined and secure manner in order to strengthen the ability of the EU, a state, an administration, or a private organisation to act independently and to have final decision-making authority regarding its processes and activities. Digital sovereignty should be consistently aligned with the specific risk constellation of the respective application context and oriented towards technologically and economically competitive solutions. Sovereignty requirements should rely on international benchmarking and pursue a leadership ambition.

Enhancing digital sovereignty therefore aims to reduce critical dependencies and to foster the active development, promotion and protection of key technological areas as well as the capability and capacity to strategically develop and deploy own products and innovations. Reduction of dependencies should not lead to isolation and should go hand in hand with partnerships with trusted international partners, provided that these partners meet our requirements for digital sovereignty. Those partnerships are a crucial instrument in this context. It will be important to ensure that European actors and governments retain access to state-of-the-art digital solutions.

2 Application logic

This paper provides a modular and scalable framework. It defines digital sovereignty based on different weightings and the potential accumulation of individual dimensions. Strengths in one dimension can – depending on the context – compensate deficits in others, allowing for a differentiated and pragmatic assessment while supporting technological competitiveness and strategic positioning.

This requires a risk-based approach: in critical environments with elevated risk levels, sovereignty requirements with regard to digital services or products need to become more relevant. This risk-based approach therefore also implies gradual sovereignty considerations corresponding to the criticality of the respective product or service cluster and, where such differentiation is necessary, components. This enables proportionate application, supports economic efficiency, and avoids any unnecessary administrative burden while preserving room for innovation.

In this context, the practical application of digital sovereignty combines both defensive and proactive components. Together, these two complementary dimensions ensure that the definition of digital sovereignty is not only focussed on the protection against risks, but also on the active development of European capabilities and competitiveness.

3 Application criteria

This legally non-binding paper proposes a framework built around six core dimensions that describe requirements of digital sovereignty and specify the abstract definition. Each building block defines a set of criteria and is designed to address a specific risk or policy objective related to digital sovereignty. The six building blocks are complementary.

The six dimensions of digital sovereignty developed in Section 3 fall into three categories: Foundational Dimensions of Digital Sovereignty (3.1 & 3.2), Economic Capabilities (3.3) and Technical and Systemic Capabilities (3.4 – 3.6).

Foundational Dimensions of Digital Sovereignty

3.1 Capability to implement and enforce: The EU, Member States and other users of digital products and services can effectively implement and enforce their conditions for securing digital sovereignty with economic, legal and political instruments, provided they are respecting the EU's international trade commitments (especially free trade agreements, FTA), e.g. through the following measures:

- Use of digital products or services from a provider whose top-holding company is headquartered in an EU Member State or, under certain risk-based conditions, in a trusted international partner state.
- Ensuring compliance with EU law as a foundation for the effective enforcement of EU law and security standards.
- Transparency regarding percentage of ownership share including subcontractor chains.
- Disclosure of existing economic, legal and technical dependencies on third countries while safeguarding business and trade secrets.
- Creating legal and technical preconditions to effectively conduct criminal investigations and legal proceedings against cybercriminals, state-sponsored attackers, and other actors who threaten digital infrastructure.
- Legal and technical restriction of such extraterritorial data access and outflow that is critical to sovereignty.
- International rules and (technology) standards, open source standards in particular, can ensure the interchangeability and adaptability of technologies, create equal conditions and prevent negative developments.

3.2 The capability to design, deploy and use technologies: Industry, scientists, developers and users master digital technologies in terms of research, development and application, for example through:

- Availability of a scientific ecosystem that can take the lead in key digital technologies (e.g. artificial intelligence, microelectronics, robotics, data, quantum technologies, cybersecurity).
- Promotion of industrial demand for key digital technologies.
- Promotion and funding of research and knowledge transfer between science and users in the economy, administration and civil society, e.g. in the form of joint research, exchange formats, re-usability of developed solutions, intersectoral mobility, training, documentation and knowledge management.
- Promotion of market entry of R&D and innovation, and scaling up of digital start-ups including by providing better access to financial markets (including venture capital) to support growth and stimulating the capability of European companies in key technological areas to innovate.
- Possibility of direct technical co-creation by users, especially via open source, open hardware and open access, as well as interoperability within systems and suitable interface standards, where applicable, and participation of users and workers' representatives when technologies are introduced at the workplace.
- Promotion of research and development cooperation in key digital technologies within the EU and, after weighing risks and opportunities, with trusted international partners, as well as taking into account national and European research security frameworks.
- Availability of sufficient capacities and competencies for purchase, development and operation of digital solutions (including analysis of systemic dependencies of existing systems), particularly in the area of security and defence industrial key technologies.
- Providing capacities and capability in the relevant standardisation bodies for the respective technologies.

Economic Capabilities

3.3 Economic Value Creation Capability and Capacity

Actors across the EU knowledge and value chains should develop and foster globally scalable digital services, products and infrastructures. This framework aims at helping create a virtuous circle by stimulating

demand for sovereign solutions through a toolbox for strategic public procurement, supporting investment and skilled employment within the EU, and supporting the development of a domestic ecosystem. Such solutions can also include partial value creation in trusted third partner countries. The framework aims at anchoring R&D, talent development and technological expertise in Europe, strengthening European capabilities, and contributing in the long term to reducing strategic dependencies. It aims at maintaining the European potential for innovation and its technological edge.

The following indicators aim to measure the share of value added generated within the EU of a digital service or product and to assess the territorial anchoring of activities:

- Contribution to the economic development of the European ecosystem: development, use, scaling and dissemination of sovereign technology (hardware/software), IT solutions and promoting sovereign digital services (suppliers) that create measurable economic value within EU/EEA, incentivise European innovation ecosystems, and enhance Europe's technological and industrial capability while remaining compatible with an open and competitive market approach, including solutions from trusted international partners. For example, a digital service's predominant reliance on European technology suppliers may illustrate its contribution to the local ecosystem and mitigation of risks by showing the extent to which it supports and strengthens the European technological value chain.
- Contributing to the technological development, influence and sovereignty of the EU: Ensuring the availability, within the EU, of a scientific and innovation ecosystem with dynamic competition that can take the lead in key digital technologies and independently develop, deliver and innovatively market them, aligned with international benchmarking references (e.g. in the areas of artificial intelligence, microelectronics, robotics). For example, for a digital service, this could be reflected by examining whether key R&D and engineering capabilities, including core development and critical support functions, are located in the EU, thus mitigating risks.
- Stimulating European skilled workers employment: Employee location, R&D location and place of operational control may be considered as indicators to measure skilled employment.
- Strengthening basic digital literacy of European citizens to ensure the independent, self-determined and secure use of digital services and technologies.

A European ecosystem also requires strategic state investment, partnerships that secure market access, and protection of technologies, companies, and personnel against security-relevant third-country takeover, harmful influence, or extraterritorial regulation.

Technical and Systemic Capabilities

3.4 Protection of Data: Safeguarding the most sensitive data and control of digital technology is indispensable to foster economic stability and growth as well as innovation in Europe. This paper calls on the European Commission to define highest protection standards for the most sensitive data, including adequate safeguards to protect data from cybersecurity risks and the effects of non-EU extraterritorial legislation, and mandatory usage of privacy-enhancing technologies.

3.5 Substitutability and Interoperability of Systems: Systems' designs allow for technological decisions that do not cause any unilateral dependencies on states or economic actors, but rather enable a change of provider and technology within reasonable time and financial expenditure. Open source solutions can and should play an important role in this regard. Characteristics for substitutability and interoperability could include:

- Modular design of architectures used throughout the IT stack and for entire systems.
- Use of systems with open (where applicable: free) data standards and interfaces (free licences/open source, e.g. supplemented by international norms and standards, NATO standards).
- Introduction of corresponding requirements regarding modularity, open interfaces and data standards within the European framework to enable interchangeability within Europe.

- Creating transparency in the supply chain, in particular through complete and traceable documentation of software codes, components and interfaces in the form of an SBOM (Software Bill of Materials).
- Designing migration paths, technical, economic and legal exit concepts, and multi-vendor strategies.

3.6 Infrastructure Resilience: This dimension aims at the development and operation of trustworthy critical IT infrastructures, which will be performed under domestic control and will in future primarily rely on solutions from EU Member States. This dynamic towards a more competitive European digital value chain can be supported through cooperation with trusted international partners:

- Establishment and strengthening of computing infrastructures (especially in the areas of artificial intelligence, quantum computing and cloud computing) and availability of sufficient sovereign data centres, strategic allocation of appropriate sites, and competitive energy prices in EU Member States.
- Establishment and strengthening of sovereign and interchangeable hard- and software stacks in the European Union, and also from trusted international partner states.
- Establishment of an adequate level of security for the respective application.
- Securing the prerequisites for resilient infrastructures, in particular through the availability of necessary IT components via diversified and reliable supply chains, as well as through the development and maintenance of necessary IT competencies within the framework of strategic personnel development.
- Availability and utilisation of secure, safe and sustainable energy, such as renewable energy, combined with a commitment to optimise life-cycles of the hardware infrastructure to ensure long-term resource independence.
- Availability of comprehensive high-performance networks.
- Ensuring access to critical space resources (satellite communication, earth observation, navigation systems).