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).

Mise en garde : Ce document ne vise pas à traiter de questions relatives à la défense et à la sécurité nationale, dont les caractéristiques particulières exigent un cadre spécifique. Conformément à l'article 4, paragraphe 2, troisième phrase, du Traité sur l'UE, ces domaines relèvent de la seule responsabilité des États membres.

Note : Le présent document a un caractère politique et expose les grandes lignes de la conception commune qu'ont la France et l'Allemagne de la souveraineté numérique. À ce titre, il vise à stimuler et orienter les débats et les travaux législatifs qui seront menés à l'échelle européenne.

1 Objectif général

Il est urgent d'agir

La souveraineté numérique européenne doit être renforcée en réduisant les dépendances critiques à l'égard de technologies, de ressources, de produits et de services numériques provenant de pays tiers. Ces dépendances critiques existent à tous les niveaux de la pile technologique, des infrastructures informatiques (y compris les semi-conducteurs) et des logiciels au traitement de données et à l'intelligence artificielle, et dans tous les secteurs.

La souveraineté numérique de chaque État membre est inextricablement liée à la souveraineté numérique de l'Europe. S'il est vrai que des mesures doivent être mises en œuvre au plan national, il n'en demeure pas moins nécessaire d'instaurer une coordination et une coopération autour d'objectifs clairs à l'échelle européenne pour garantir une souveraineté numérique complète et durable. L'Europe aspire à une transformation numérique fondée sur des valeurs, des normes et des intérêts communs, qui lui permettrait de se positionner en tant qu'acteur indépendant au sein de l'économie mondiale et la concurrence géopolitique.

Compte tenu des récents bouleversements géopolitiques et de la concurrence systémique croissante, il est crucial d'assurer des zones d'influence stratégique européenne, de réduire les dépendances et les vulnérabilités stratégiques et d'éviter l'enfermement propriétaire. Dans le monde entier, les technologies numériques sont désormais au cœur des chaînes de valeur économiques et de la compétitivité. Le rapport Draghi établit un lien clair entre la souveraineté numérique et la stabilité économique. La souveraineté numérique est donc essentielle à la sécurité économique.

Au regard de la situation géopolitique, la souveraineté numérique est plus que jamais un enjeu majeur de sécurité. Les cyberattaques, les failles de sécurité, le cyberespionnage et les menaces hybrides visent de manière croissante des infrastructures numériques qui sont les systèmes nerveux de nos démocraties, nos économies et nos sociétés. Des perturbations dans la chaîne d'approvisionnement, celle des puces électroniques par exemple, peuvent se produire n'importe où dans le processus de fabrication. Elles pourraient conduire à des arrêts de production chez certains fournisseurs clés et menacer la disponibilité du matériel nécessaire. Parallèlement, l'ouverture des marchés et la coopération internationale avec des partenaires de confiance continuent d'être des piliers essentiels de la souveraineté numérique européenne.

Par ailleurs, le renforcement de la souveraineté numérique implique également de créer les conditions nécessaires pour mener efficacement des enquêtes et des poursuites pénales à l'encontre des cybercriminels, des attaquants étatiques et d'autres acteurs qui menacent les infrastructures numériques. Le renforcement de la souveraineté numérique européenne permet donc de veiller à ce que la création de valeur européenne soit indissociable de la sécurité.

Accroître la souveraineté numérique de l'UE ne signifie pas se tourner vers le protectionnisme et l'isolationnisme ; les États membres européens entendent ainsi poursuivre leur coopération avec des partenaires internationaux de confiance, c'est-à-dire en particulier des partenaires qui respectent les droits de l'homme, les principes démocratiques et l'État de droit et satisfont aux principes fondamentaux en matière de protection des données. En outre, les obligations juridiques internationales découlant de traités bilatéraux ou multilatéraux et d'accords de libre-échange devront être respectées et exécutées.

Dans le cadre de systèmes de sécurité collectifs, la principale priorité devrait résider dans une capacité d'action commune afin de garantir le dispositif de dissuasion et de défense collectives de l'Alliance. À la lumière de l'article 4, paragraphe 2, troisième phrase, du TUE, il est indiqué expressément que ce document ne vise pas à traiter de questions relatives à la défense et à la sécurité nationale.

Par ailleurs, ce document ne vise en aucun cas à imposer des conditions en matière d'achats à des entreprises du secteur privé, mais il peut leur offrir des outils pour évaluer leurs dépendances et assurer le suivi de leurs approvisionnements.

Enfin, ce document ne crée aucune obligation d'investissement à l'égard d'un État membre de l'UE ni n'entraîne plus généralement de dépenses publiques supplémentaires. Si les critères exposés dans ce document doivent être appliqués dans le contexte des dépenses publiques, cela s'effectuera sous réserve de l'approbation des financements conformément aux principes pertinents du droit budgétaire, les crédits budgétaires étant alloués dans le cadre de la procédure d'élaboration du budget correspondante. Les principes de proportionnalité et d'efficience sont applicables.

Une stratégie ambitieuse

L'Europe a besoin de renforcer son écosystème numérique en se fondant à la fois sur des initiatives lancées au niveau européen et sur des projets innovants impulsés au niveau national, et en respectant le principe de subsidiarité de manière à garantir l'affectation la plus efficace des ressources et des responsabilités. La technologie numérique est au cœur de la plupart des chaînes de valeur et donc de la croissance économique ; les dépendances en la matière exposent les économies à des vulnérabilités systémiques qui affaiblissent à long terme la capacité de l'UE à prendre des décisions souveraines.

La plupart des entreprises européennes du numérique emploient moins de 250 salariés[1]. Bien qu'innovantes, elles ont du mal à changer d'échelle. En l'absence d'une action ciblée, l'Europe risque de rester un continent innovant caractérisé par une insuffisance d'acteurs économiques opérant à l'échelle mondiale. La stratégie de l'Europe reflète son ambition de renforcer son rôle de producteur, de normalisateur et d'artisan du développement technologique.

Ce document propose un cadre commun visant à renforcer la capacité de l'Europe à être un acteur dans le domaine du numérique, en combinant résilience, compétitivité et capacités technologiques. Il comporte des mesures à la fois défensives et proactives. Les mesures défensives sont destinées à protéger l'Europe contre les mesures de coercition étrangères (que ce soit par des moyens légaux ou des restrictions technologiques), à sauvegarder les actifs stratégiques et à protéger les données sensibles. Les mesures proactives, quant à elles, visent à favoriser la capacité de l'Europe à prendre des décisions de manière indépendante en se fixant des objectifs dans les domaines de l'éducation, de la recherche, de l'innovation et de la sécurité économique. Un autre objectif de ces mesures proactives est de renforcer les chaînes de valeur européennes en apportant un appui au développement, au déploiement et à l'utilisation d'infrastructures, de technologies et de services numériques. L'objectif de ce document conjoint est de promouvoir une réponse européenne politique cohérente et opérationnelle.

Il vise également à alimenter les réflexions que mène actuellement la Commission européenne sur les différents véhicules législatifs qui seront discutés en 2026 (notamment le Paquet souveraineté technologique qui comprend entre autres la proposition de règlement sur le développement de l'informatique en nuage et de l'IA) et au-delà, tout en apportant, pour les années à venir, une vision de long terme de la souveraineté numérique européenne.

Compte tenu de son objectif qui est de définir les composantes et les critères de la souveraineté numérique, et de tenter d'en faire un concept aussi opérationnel que possible, ce document pourrait également constituer pour l'écosystème numérique européen un cadre de référence volontaire d'évaluation de ses vulnérabilités en la matière.

[1] Commission européenne/ JRC, *Annual Report on European SMEs 2024/2025*, Tableau 17 ("Industrial Ecosystems: Proportion of Economic Activity by Size Class (2024)"), ligne "Digital".

Définition

La souveraineté numérique désigne la capacité de développer, fournir, utiliser, adapter et contrôler des technologies numériques, y compris des matériels, de manière indépendante, autonome et sûre, afin de renforcer la capacité de l'UE, d'un État, d'une administration ou d'une entité privée à agir de manière indépendante et à disposer du pouvoir ultime de décision en matière de processus et d'activités. La souveraineté numérique doit être cohérente avec le paysage des risques spécifique au domaine d'application, et fondée sur des solutions technologiques et économiques compétitives. Les exigences en matière de souveraineté doivent reposer sur des comparaisons internationales et répondre à une stratégie ambitieuse garantissant une position de chef de file à l'Europe.

Renforcer la souveraineté numérique vise par conséquent à réduire les dépendances critiques et à favoriser de manière proactive le développement, la promotion et la protection des secteurs technologiques essentiels, ainsi qu'à augmenter la capacité et les moyens permettant de développer et de déployer de manière stratégique les innovations et produits européens. La réduction des dépendances ne doit pas conduire à l'isolationnisme et doit s'accompagner d'une coopération avec des partenaires internationaux de confiance, dès lors qu'ils remplissent nos exigences en matière de souveraineté numérique. Dans ce contexte, ces partenariats sont fondamentaux. Il sera également essentiel de garantir que les acteurs et gouvernements européens continuent à avoir accès aux solutions numériques de pointe.

2 Stratégie de mise en œuvre

Ce document propose un cadre modulaire et évolutif. Il définit la souveraineté numérique en se fondant sur des critères et des catégories de composantes. Les forces au niveau d'une composante peuvent, selon le contexte, compenser des insuffisances à d'autres niveaux, ce qui permet de procéder à une évaluation différenciée et pragmatique tout en soutenant la compétitivité technologique et un positionnement stratégique.

Une approche fondée sur les risques est à cet égard nécessaire : dans des environnements critiques présentant des niveaux de risque élevés, les exigences en matière de souveraineté s'agissant des services et produits numériques doivent devenir plus pertinentes. Cette approche implique donc également une graduation des exigences, en fonction du caractère critique du groupe de produits ou de services en question, voire des composantes. Cette graduation permet une mise en œuvre proportionnée, favorise l'efficacité économique et évite une charge administrative inutile, tout en ménageant une marge de manœuvre pour l'innovation.

La mise en œuvre de la souveraineté numérique combine donc des mesures à la fois défensives et proactives complémentaires qui garantissent que la définition de la souveraineté numérique est non seulement axée sur la protection contre les risques, mais aussi sur le développement actif des capacités et de la compétitivité européennes.

3 Critères de mise en œuvre

Ce document juridiquement non contraignant propose un cadre fondé sur six composantes de la souveraineté numérique et qui précise sa définition. Chacune regroupe un ensemble de critères et recouvre un risque ou un objectif politique spécifique en lien avec la souveraineté numérique. Ces six composantes sont complémentaires.

Les six composantes de la souveraineté mentionnés au point 3 sont classés en trois catégories : les composantes fondamentales de la souveraineté numérique (points 3.1. et 3.2.), la capacité à créer de la valeur économique et les moyens d'y parvenir (point 3.3.) et les capacités techniques et des systèmes (points 3.4 à 3.6).

Composantes fondamentales de la souveraineté numérique

3.1 Capacité à mettre en œuvre et à faire respecter la souveraineté numérique : l'UE, les États membres et d'autres utilisateurs de produits et services numériques peuvent mettre en œuvre et faire respecter de manière effective leurs propres instruments économiques, juridiques et politiques pour garantir la souveraineté numérique, sous réserve du respect des engagements de l'UE en matière de commerce international (notamment des accords de libre-échange – ALE), en adoptant par exemple les mesures suivantes :

- Utiliser des produits ou services numériques d'un fournisseur dont la société holding de tête a son siège dans un État membre de l'UE ou, dans certaines conditions fondées sur une évaluation des risques, dans un État partenaire de confiance.
- Faire de la conformité à la législation de l'UE le fondement qui permette de faire respecter le droit et les standards de sécurité européens de manière effective.
- Assurer la transparence concernant la quote-part de détention du capital, y compris dans les chaînes de sous-traitance.
- Divulguer l'existence de liens de dépendance économique, juridique ou technique à des pays tiers, tout en préservant le secret professionnel et le secret des affaires.
- Créer les conditions juridiques et techniques préalables qui sont nécessaires pour mener efficacement des enquêtes et des poursuites pénales à l'encontre des cybercriminels, des attaquants étatiques et d'autres acteurs qui menacent les infrastructures numériques.
- Imposer des restrictions juridiques et techniques aux consultations et aux transferts extraterritoriaux de données qui revêtent une importance critique du point de vue de la souveraineté.
- Mettre en place des règles et des standards (technologiques) internationaux, en particulier des standards ouverts, pouvant garantir le développement de technologies interchangeables et adaptables, assurer l'égalité de traitement et prévenir les événements indésirables.

3.2 Capacité à concevoir, à déployer et à utiliser les technologies : les acteurs du secteur, les scientifiques, les développeurs et les utilisateurs peuvent maîtriser les technologies numériques, dans les domaines de la recherche, du développement ou des applications, grâce notamment aux mesures suivantes :

- Mettre en place un écosystème scientifique capable de jouer un rôle de premier plan dans le domaine des technologies numériques clés (par exemple, l'intelligence artificielle, la microélectronique, la robotique, les données, les technologies quantiques ou la cybersécurité).
- Susciter une demande de l'industrie pour les technologies numériques clés.
- Promouvoir et financer la recherche et le transfert de connaissances entre les acteurs scientifiques et les utilisateurs dans la sphère économique, l'administration et la société civile, par exemple sous la forme de projets de recherche communs, de formats d'échange, de solutions réutilisables, d'une mobilité intersectorielle, de formations ou d'une gestion documentaire et des connaissances.
- Promouvoir l'entrée sur le marché d'acteurs de la R-D et de l'innovation, et favoriser l'expansion des start-ups du numérique, notamment en assurant un meilleur accès aux marchés financiers (y compris au capital-risque) pour soutenir la croissance et stimuler la capacité d'innovation des entreprises européennes opérant dans des domaines technologiques clés.
- Donner aux utilisateurs des possibilités de cocréation technique directe, en particulier par le biais du logiciel libre (*open source*), du matériel libre (*open hardware*) et de l'accès libre (*open access*), prévoir l'interopérabilité des systèmes et des standards d'interfaces adaptés, le cas échéant, et promouvoir la participation de représentants d'utilisateurs et de salariés lorsque des technologies sont introduites dans l'environnement professionnel.
- Promouvoir la coopération en matière de recherche-développement dans les technologies numériques clés au sein de l'UE mais aussi, après avoir évalué les risques et les opportunités, avec des partenaires internationaux de confiance, en tenant également compte des cadres nationaux et européen en matière de sécurité de la recherche.
- Faire en sorte de disposer de compétences et de moyens suffisants pour acquérir, développer et exploiter des solutions numériques (y compris concernant l'analyse des dépendances systémiques existantes), en particulier dans le domaine des principales technologies industrielles de sécurité et de défense.
- Fournir des moyens et des capacités aux organismes de normalisation qui sont compétents pour les technologies en question.

Capacités économiques

3.3. Capacité à créer de la valeur économique et moyens d'y parvenir

Les acteurs des chaînes de valeur et des connaissances de l'UE devraient développer et promouvoir des services, des produits et des infrastructures capables de prendre une envergure mondiale. Le présent cadre vise à contribuer à créer un cercle vertueux par la stimulation de la demande en solutions souveraines grâce à des outils permettant d'effectuer des achats publics stratégiques, par le soutien aux investissements et à l'emploi qualifié au sein de l'UE et par la contribution au développement d'un écosystème européen. De telles solutions peuvent également intégrer la création d'une partie de la valeur ajoutée dans des pays partenaires de confiance hors de l'UE. Le cadre a pour objectif d'enraciner les activités de recherche-développement, le développement des talents et l'expertise technologique en Europe, de renforcer les capacités européennes et de contribuer, à long terme, à réduire les dépendances stratégiques. Il ambitionne de préserver le potentiel européen d'innovation et l'avantage technologique de l'Union.

Les indicateurs présentés ci-dessous visent à mesurer la part de la valeur ajoutée d'un produit ou d'un service numérique créée au sein de l'UE, et à évaluer l'ancrage territorial des activités :

- contribuer au développement économique de l'écosystème européen : développer, utiliser, faire passer à l'échelle et diffuser des technologies (matérielles et logicielles) et des solutions informatiques souveraines, et favoriser l'émergence de services numériques et de fournisseurs de

services numériques souverains qui créent une valeur économique mesurable dans l'UE/EEE, stimulent les écosystèmes d'innovation européens et renforcent les capacités industrielles et technologiques de Europe, tout en restant compatibles avec une approche de marché libre et concurrentielle. Cela peut également passer par l'adoption de solutions de partenaires internationaux de confiance. À titre d'exemple, un service numérique qui s'appuierait principalement sur des fournisseurs de technologies européens permettrait d'illustrer sa contribution à l'écosystème local et à l'atténuation des risques en montrant à quel point il soutient et renforce la chaîne de valeur technologique européenne ;

- contribuer au développement, à l'influence et à la souveraineté technologiques de l'UE : garantir, au sein de l'UE, la disponibilité d'un écosystème scientifique et d'innovation caractérisé par une concurrence dynamique capable de jouer un rôle de premier plan dans le secteur des technologies numériques clés, de les développer et de les déployer en toute indépendance ainsi que de les commercialiser d'une manière innovante, conformément aux référentiels internationaux (par exemple, dans le domaine de l'IA, de la microélectronique et de la robotique). À titre d'exemple, dans le cas d'un service numérique, cela pourrait se traduire par la vérification de la présence, au sein de l'UE, de capacités essentielles en matière de recherche-développement et d'ingénierie, y compris les fonctions principales de développement et les fonctions indispensables d'appui, ce qui permettrait d'atténuer les risques ;

- stimuler l'emploi des travailleurs qualifiés européens : utiliser, le cas échéant, le lieu de travail, l'emplacement des activités de recherche-développement et le lieu d'exercice du contrôle opérationnel comme des indicateurs pour mesurer le niveau de l'emploi qualifié ;

- augmenter le niveau élémentaire de littératie numérique des citoyens européens afin de garantir un usage indépendant, autonome et sécurisé des services et des technologies numériques.

Un écosystème européen requiert également des investissements et des partenariats stratégiques de l'État pour assurer l'accès au marché et la protection des technologies, des entreprises et des salariés contre la mainmise de pays tiers, des influences préjudiciables et l'application d'une réglementation extraterritoriale en matière de sécurité.

Capacités techniques et des systèmes

3.4 Protection des données : La protection des données les plus sensibles et la maîtrise des technologies numériques sont indispensables pour favoriser la stabilité économique et la croissance ainsi que l'innovation en Europe. Ce document invite la Commission européenne à définir des normes de protection extrêmement strictes pour les données les plus sensibles, incluant des mesures adéquates de protection contre les risques de cybersécurité et les effets de l'application extraterritoriale de législations adoptées hors de l'UE, ainsi que des obligations de mise en œuvre de technologies de protection de la vie privée.

3.5 Substituabilité et interopérabilité des systèmes : Les systèmes doivent être conçus de sorte que les choix technologiques ne produisent aucune dépendance unilatérale vis-à-vis d'un État ou d'un acteur économique, mais permettent au contraire de changer de fournisseur et de technologie dans un délai raisonnable et sans dépenses excessives. Des solutions open source peuvent et devraient jouer un rôle important à cet égard. Les caractéristiques de substituabilité et d'interopérabilité pourraient inclure :

- Une conception modulaire des architectures de toute la pile technologique et des systèmes dans leur globalité.
- L'utilisation de systèmes reposant sur des normes en matière de données et des interfaces ouvertes (gratuites lorsque cela est possible) (licences libres/open source, complétées par exemple par des normes et standards internationaux, notamment les normes de l'OTAN).
- L'introduction d'exigences correspondantes concernant la modularité, les interfaces ouvertes et les normes en matière de données dans le cadre européen pour permettre l'interchangeabilité dans les frontières de l'UE.

- La transparence de la chaîne d'approvisionnement, notamment par une documentation complète et traçable des codes logiciels, des composants et des interfaces, sous la forme d'une nomenclature logicielle (*Software Bill of Materials*, SBOM).
- La conception de voies d'évolution, de principes de sortie des dépendances techniques, économiques et juridiques, ainsi que de stratégies multifournisseurs.

3.6 Résilience des infrastructures : Cette composante a pour objet le développement et l'exploitation d'infrastructures numériques critiques fiables, qui se feront sous contrôle national et qui reposeront essentiellement sur des solutions basées dans l'UE. Cette évolution vers une chaîne de valeur numérique européenne plus compétitive peut être favorisée par une coopération avec des partenaires internationaux de confiance.

- Mise en place et renforcement d'infrastructures de calcul (en particulier dans les domaines de l'IA, du calcul quantique et de l'informatique en nuage) et disponibilité d'une capacité suffisante de centres de données souverains, répartition stratégique des sites adéquats et prix de l'énergie compétitifs dans les États membres.
- Mise en place et renforcement de piles technologiques matérielles et logicielles souveraines et interchangeables dans l'UE ainsi qu'en partenariat avec des États partenaires de confiance.
- Mise en place d'un niveau de sécurité adéquat pour chaque application concernée.
- Garantie des conditions nécessaires aux infrastructures résilientes, notamment la disponibilité des composants informatiques indispensables fournis par des chaînes d'approvisionnement diversifiées et fiables, ainsi que le développement et la consolidation des compétences numériques requises à l'intérieur d'un cadre stratégique de développement des talents.
- Disponibilité et utilisation de ressources en énergie sécurisées, sûres et durables, telles que les énergies renouvelables, en corrélation avec un engagement à optimiser les cycles de vie des infrastructures matérielles afin d'assurer une indépendance à long terme en matière de ressources.
- Disponibilité de réseaux intégrés haute performance.
- Garantie d'un accès aux ressources de l'espace essentielles (communication par satellite, observation de la Terre, systèmes de navigation).