Accelerating together towards European technological sovereignty

Executive summary

Achieving technological sovereignty is a core responsibility of national governments and the European Commission, which must act on behalf of the entire EU. While companies play a crucial role in this process, their primary objective remains global competitiveness and long-term market success, which depend on innovation and resilience in the face of adverse conditions. Political sovereignty and industrial competitiveness must, however, go hand in hand in today's increasingly complex geopolitical environment. It is therefore essential to focus on measures that deliver sustainable benefits for both policymakers and industry.

The **French Business Confederation (MEDEF), the Federation of German Industries (BDI)** and **The Confederation of German Employers' Associations (BDA)** believe that technological sovereignty has become a central pillar of Europe's future. Sovereignty is not about withdrawing from global co-operation and should not lead to isolation, but rather **strengthen our ability to take self-determined decisions**, **choose our partners freely**, and **protect strategic interests of European companies**. Our Policy Makers have the responsibility to create the right framework conditions, such as competitive energy prices, access to skilled labor, reduced bureaucracy, accelerated permitting, and a vibrant capital market, that enable companies to thrive and contribute to Europe's sovereignty. Our ambition is to ensure that France, Germany and the European Union can also rely on credible, competitive, and trusted **technological alternatives** developed within our own digital **ecosystems**. While reducing dependencies, Europe also needs a proactive approach that builds on its industrial strengths and innovation potential. Europe should lead the development of next-generation digital technologies by focusing on strategic fields such as industrial AI, microelectronics, robotics, advanced materials, secure infrastructures, cybersecurity, and sovereign data spaces, while fostering an integrated innovation ecosystem that accelerates research, commercialization, and scale-up.

To achieve this, we must reinforce our capacity to act independently across entire value chains, spanning from infrastructure, semiconductors, AI and cybersecurity to law, innovation, and talent. While sovereignty ultimately remains the prerogative of states, it

also relies on the commitment and capability of businesses. We therefore encourage public and private stakeholders to work together with renewed ambition to develop a truly sovereign, open, and ambitious European digital model.

Today, our **technological dependencies** are alarming, as Europe produces less than ten percent of global semiconductors. Our submarine cables, vital for Internet traffic, often fall outside our control. These dependencies threaten not only our industrial competitiveness but also our capacity to act with full strategic confidence and independence.

It is essential that Europe responds to this challenge with unity, determination, and a clear vision for its digital future. This means strengthening our strategic capacity and progressively reducing **dependencies in the digital space,** just as we have begun to do in the energy and defense sectors. It also means fostering an open **single market**, **defending our values**, and **creating conditions that allow new European champions and industrial ecosystems to emerge, especially through fostering AI ecosystems and increasing AI diffusion to secure economic prosperity**. Sovereignty is not about closing borders: On the contrary, it is about regaining control over our choices.

We therefore propose a strategy focused on **six priorities**:

1. Infrastructures

Digital infrastructures – such as data centers, submarine cables, and network connectivity – and enabling technologies like semiconductors form the digital foundation of our modern economy. Yet, Europe remains critically dependent on non-European actors. For example, U.S cloud providers dominate the market, Europe's chip production covers less than ten percent of global output, and submarine cable control escapes EU's hands. These dependencies limit Europe's capacity to act with confidence and safeguard its strategic priorities. The fragmented governance and slow implementation of the EU's programs further undermine strategic coherence.

Infrastructure must be understood not only as physical production capacity, but also as the intellectual and technological foundations that enable innovation. This includes strategic semiconductor R&D to advance chip design, reduce dependencies, and secure Europe's role globally. While infrastructure alone cannot create sustainable adoption, it can accelerate it where industry use cases show real demand.

Without sovereign and secure infrastructure, Europe is vulnerable to disruption and geopolitical pressure.

Consequently, French and German industry believe that improving digital and technological sovereignty requires urgent investment and coordination to secure critical assets, ensure economic resilience and maintain competitiveness in the global race for innovation. In addition to physical infrastructures, Europe must secure strategic research and technology infrastructures, IP governance systems and trusted data spaces as core components of technological sovereignty.

2. Cybersecurity

According to most recent data, 87 % of German companies have been attacked with the aim of data theft, industrial espionage or sabotage, whereas in France cyber-attacks to companies grew 15 percent between 2023 and 2024. European businesses are structurally vulnerable to growing cyber threats by being exposed to risk-prone supply chains. Rather than having to fulfil overly bureaucratic regulatory requirements, the European co-legislators must reduce reporting obligations and thereby free resources within companies for risk mitigating measures and incident mitigation. Nearly half of them experienced at least one successful attack in 2024, with both large corporations

and SMEs facing ransomware, data theft and industrial espionage. The cybersecurity landscape remains fragmented across the EU, with divergent national regulations and certifications hindering the emergence of cohesive European solutions.

SMEs are especially exposed as most of them feel unprepared for cyberattacks, and their limited resources put their survival at risk. Many SMEs go bankrupt following a major incident. This lack of protection directly undermines economic resilience and competitiveness.

In this context, cybersecurity must become a cornerstone of Europe's digital sovereignty. Trust in digital services, business competitiveness, and strategic autonomy all depend on the ability to secure critical infrastructure. Without cyber resilience, there can be no lasting sovereignty in an increasingly contested digital world. To enhance Europe's resilience against cyber threats, the EU must establish a real-time situational awareness system daily situation picture based on incident reports and intelligence. Another key factor for European sovereignty lies in cyber-secure supply chains. A standardized toolbox that recognizes CRA conformity assessments, integrates risk assessments in accordance with the NIS 2 Directive, and is based on the zero-trust principle can help manufacturers and integrators systematically raise their security standards. Close cooperation with trusted international partners is essential to strengthen global cybersecurity and build resilience against cross-border threats.

However, it is important to emphasize that ensuring a high and harmonized level of cybersecurity across the European territory should not preclude the need for proportionate obligations. In order for cybersecurity to become a competitive advantage for European companies and a pillar of our sovereignty, we must ensure that the regulatory framework for cybersecurity remains coherent and proportionate, and that different regulations do not create overlapping or redundant obligations.

The EU must invest in the protection of digital and critical infrastructure and fostering strategic partnerships with European cybersecurity companies. Furthermore, Cybersecurity has to be embedded in a broader concept of research and innovation security as an enabler of technological sovereignty, ensuring project-level risk management, IP governance and European minimum standards for secure research environments. To ensure long-term protection, the EU should also consider and promote the implementation of Post-Quantum Cryptography standards across critical infrastructure and digital services.

3. Artificial Intelligence and Cloud

Artificial Intelligence (AI) is a cornerstone for achieving technological sovereignty in Europe. Currently, the EU remains highly dependent on third countries in critical AI

domains, including advanced foundation models (LLMs), AI chips, and cloud infrastructure. These dependencies can pose significant geopolitical risks and hinder the development of independent European solutions. Fragmented regulation, particularly in data protection, creates legal uncertainty and stifles innovation, especially for start-ups and SMEs. This is also true for the AI Act, which has created double regulations, particularly in the realm of industrial AI and medical devices, while simultaneously posing grave challenges for regulators and notified bodies due to overly optimistic timelines. At the same time, limited access to high-performance computing infrastructure andventure capital and limited availability of energy and high energy prices constrain the AI diffusion in general and scaling of European AI companies.

To strengthen Europe's competitiveness and resilience, the EU should focus on leveraging its unique strengths: Europe should promote sectoral specialisation and application-driven AI solutions across all industries, particularly healthcare, energy, manufacturing, mobility, finance, and the public sector. Expanding digital infrastructure, including data centers beyond Gigafactories and AI Factories, is essential to enable both frontier AI research and large-scale AI deployment in industry. In addition, edge AI should form an integral part of Europe's AI infrastructure, which enables decentralized, real-time processing close to the source of data. European companies already hold a competitive edge in embedded systems and industrial applications, which can translate into cross-sectoral advantages in mobility, manufacturing, robotics, and energy. Europe needs a dual approach: fostering excellence in AI development and application alike.

Public institutions can act as anchor customers for sovereign data centers, thereby catalysing investment. A strategic multi-cloud approach can help reduce dependencies on non-European hyperscalers.

4. Innovative ecosystems

Europe hosts a dynamic but fragile ecosystem comprising over 35,000 early-stage companies. According to the European Commission, the continent is experiencing a higher rate of start-up creation compared to the United States. Nevertheless, European start-ups fall behind the US once it comes to scaling. Thus, the number of European unicorns was estimated at 110 in the beginning of 2025, which is significantly lower than 687 unicorns reported for the USA or 369 unicorns reported for China. This disparity can be attributed to limited venture capital availability and a fragmented capital market.

Recent years have seen Europe advance through initiatives including Digital Europe, the European Innovation Council (EIC), platforms and programs provided by the European Investment Bank (EIB), and the Chips Act. Despite this progress, these efforts remain fragmented and are not sufficient to match the competitiveness of the United States or Asia. Start-ups are critical to driving innovation and enhancing competitiveness within the

region. Achieving technological sovereignty would allow Europe to innovate in accordance with its core values such as data protection, security, and sustainability.

To accomplish this, it is essential to retain unicorns within Europe and fortify the local ecosystem, particularly by fostering collaboration with established industry leaders in strategic sectors, such as secure embedded systems, automation, aerospace, and defence. Ultimately, supporting innovative ecosystems is key to positioning Europe as a leader in tomorrow's key sectors such as AI, cybersecurity, robotics and quantum technologies, and to ensuring technological sovereignty in critical value chains such as batteries and robotics. Creative tech and games companies can be viewed as good examples of key drivers of Europe's digital sovereignty and cultural identity, advancing innovation and future skills through AI development, IP creation, and culturally rooted content, further amplified by EU cultural funding and Franco-German co-productions.

Technological sovereignty requires integrated value chains from research through prototyping to industrial production. Strengthening cross-sectoral clusters (e.g. biotech, materials, chemistry) should be part of this strategy. While supporting the startup ecosystem remains essential for fostering innovation and agility, Europe's true economic strength also lies in its Mittelstand and established industrial leaders. These sectors must equally benefit from targeted measures that boost R&D investment and enable a successful transition toward digital and sustainable business models.

To secure Europe's future, all partners must unite in finally reaching the 3% R&D investment target. Achieving this goal is not merely a matter of economic ambition. It is a decisive step toward true digital sovereignty and renewed innovative strength. Only through bold, collective investment in research and innovation can Europe shape its own technological destiny and remain competitive on the global stage.

5. Extraterritoriality of Law

In the digital age, the ability of legal frameworks to extend beyond national borders is becoming increasingly relevant. For example, legislation such as the US Cloud Act and FCPA may have implications for foreign companies, including those in Europe, when there is a connection to US jurisdiction. This situation raises considerations regarding the EU's digital sovereignty. China is also developing approaches to protect its interests internationally. To date, the European Union has taken only limited steps in response to these developments. It could therefore be beneficial for the EU to further strengthen its normative role and explore the development of legal instruments to support its values, companies, and sovereignty in the global digital environment, without imposing new regulations.

The EU should focus on applying its law with determination, revising the blocking statute, enhancing institutional coordination, and demonstrating clear political will to enforce rules in a measured way. At the same time, regulation must be simplified and clarified to avoid overburdening European businesses, and digital diplomacy should be strengthened to promote the EU's approach internationally. These measures will help reinforce Europe's normative power, protect its values and companies, and ensure resilience and competitiveness in the global environment.

6. Skills

Training people of all age groups and upskilling workers is critical for national economic success, innovation, and sovereignty. The demand for continuous learning is driven by shorter technological development cycles and skill lifespans, as well as the advantages of agile methodologies and digital learning technologies. The shortage of specialised technology professionals in the labour market means that the potential of both national and international talent must be exploited more effectively.

In addition to upskilling, there is a need to attract more women to digital and ensure the participation of older skilled workers in the labor market. Global talent mobility increases the need for France and Germany to retain its existing workforce and to boost their attractiveness for non-European experts. Sustained public investment in education and research to prevent brain drain and create secure, attractive research environments is essential to maintain competitiveness and geopolitical independence.

Our concrete strategic proposals

- Use **public sector demand** strategically to support European products and technologies, especially in security-critical areas.
- Accelerate the deployment of **data centers** in France, Germany and Europe and ensure their energy supply is secure and competitively priced. This should be complemented by promoting Edge AI as an application-focused and low-energy alternative, particularly in sectors where decentralized processing enhances efficiency and sovereignty.
- Boost and simplify **Important Projects of Common European Interest (IPCEIs)** to enhance collaboration and investment in strategic industries.
- Establish framework conditions for the **cybersecurity** industry to thrive, to fund innovation and foster the emergence of European cybersecurity champions, e.g. by targeting at implementing EU-member-state-based cyber security protection for public as well as for critical infrastructure.
- **Map dependencies and vulnerabilities** in semiconductor and raw materials supply chains and establish robust monitoring systems to anticipate and mitigate risks. Cross-sectoral global supply chain disruptions and increasingly fragmented markets due to geopolitical challenges are strategic vulnerabilities. The EU must invest in expanding production capacities and diversifying supply chains while strengthening R&D capabilities in order to create beneficial interdependencies
- Improve **coordination between European institutions**, as the current overabundance of digital regulations risks creating complexity and inefficiencies for businesses and authorities alike.
- Unlock private and institutional venture capital (VC), strengthen the European fund location, and improve exit opportunities, for example through M&A or IPOs.
- Affirm a **strong political will to enforce and simplify digital regulations feasible for businesses of all sizes**, as legal deterrence only works when enforcement is credible and consistent.
- Promote **public education policies**, including digital literacy, coding workshops, the reintroduction of advanced math education, and lower entry barriers. Career guidance should be free of stereotypes and degree programmes should be more flexible and interdisciplinary.

Imprint

Federation of German Industries (BDI) | BDA | Confederation of German Employers' Associations
Breite Straße 29, 10178 Berlin
www.bdi.eu | www.arbeitgeber.de
T: +49 30 2028-0 | T +49 30 2033-0

Lobby register number: R000534 | III/720

Mouvement des Entreprises de France – MEDEF
56 avenue des Arts
1000 Bruxelles
www.medef.fr

editorial
Polina Khubbeeva
Senior Manager Digitalisation and Innovation
T: +49 30 2028-1586
p.khubbeeva@bdi.eu

Edoardo Cozzi
EU Policy Officer
T: +33 6 17 87 17 73
ecozzi@medef.eu