19 February 2026
View the online version ›

GSIS® Global Security and Innovation Summit
HAMBURG 9-10 December 2026

Monthly Executive Briefing

organised by Hamburg Messe + Congress · IISS

Implementation challenges for the EU's digital sovereignty

GSIS® HAMBURG 9-10 December 2026 Global Security and Innovation Summit

The objective of increasing the European Union's digital sovereignty has existed for almost a decade but has recently taken on renewed importance, and is increasingly featured in EU-led initiatives pertaining to regulatory reforms, greater autonomy and digital resilience. Eighteen EU member states issued the Berlin Declaration of November 2025, which called for strengthening Europe's sovereignty in strategic technologies and innovative capabilities, and urged further action by the European Commission (EC). These efforts seek to achieve digital sovereignty in the EU by streamlining regulations, reducing the deep digital dependencies on United States-based providers, and establishing a competitive and innovative digital industry. However, rapid artificial intelligence (AI) innovation and geopolitical uncertainty risk outpacing the EU's efforts to achieve this.

- The Proposal for a Regulation for the EU Cybersecurity Act, announced in January, would prohibit the use of high-risk suppliers in key ICT sectors, representing a change from past voluntary measures. Along with the Digital Omnibus Regulation Proposal, it is the latest effort to harmonise and streamline digital regulations within the EU.
- The EU's dependency on US providers for digital services is not new. However, the unpredictability of the current US administration has revived concerns over the US CLOUD Act and affected consumer confidence in the security of European data stored by US providers.
- Creating inter-operable frameworks that are clear, enforceable and transparent will enable Europe's digital and industrial potential. However, funding and support for EU industry is urgently needed to develop further technical innovations, fill capacity gaps and cut compliance costs.

GSIS 2025 News:

- ***The first version of the conference agenda is now live and available on our website. Check back regularly for the latest updates to the programme.***
- ***Exhibitor registration for GSIS 2026 is live – secure your stand today and benefit from our exclusive early bird offer!***

39%	€221.8 MILLION	€264 BILLION
PROPORTION OF GLOBAL CYBER ATTACKS RECORDED IN 2024 THAT OCCURRED IN EUROPE	EC'S ANNOUNCED COMMITMENT TO SECURING EU STRATEGIC AUTONOMY, INNOVATIVE DATA SERVICES AND TRUSTWORTHY AI	SPENT ANNUALLY BY EUROPEAN BUSINESSES ON US-BASED DIGITAL SERVICES

Introduction

The pursuit of digital sovereignty in the EU has entered a key phase. While the concept is not new – the passage of the General Data Protection Regulation (GDPR) in 2016 can be regarded as an early assertion of the EU's regulatory power and by extension its digital sovereignty – its political significance has increased considerably. The Berlin Declaration marked a shift in tempo. Signed outside the EU institutional framework, it called for strengthened European sovereignty in strategic technologies and innovative capabilities, and urged the EC to take further action. The declaration provided a broader understanding of digital sovereignty, focusing on the EU's and member states' ability to choose their digital providers, while enabling global partnerships – a necessary shift away from misperceptions about the EU striving for complete digital independence.

Digital sovereignty for the EU comprises three interconnected pillars: harmonising and streamlining EU regulations; reducing overdependence on foreign technology providers; and creating a competitive and innovative environment for European digital leadership. However, implementing digital sovereignty is hindered by limitations in the EU's ability to streamline regulation and support innovation while keeping pace with technological change and managing geopolitical uncertainty in the EU–US relationship.

"For us [digital sovereignty] doesn't mean isolation, it means a self-determination of data, it means trust, resilience and conscious collaboration across networks and borders."

Marc-Julian Siewert, CEO, secunet Security Networks AG, at GSIS 2025

Regulatory harmonisation

Regulation is the EU's most mature tool for asserting its digital sovereignty. Efforts like the GDPR, along with the Digital Markets Act, Digital Services Act and Cyber Resilience Act, allowed it to leverage its market size to shape global data practices and improve product security. These measures placed European digital rights and principles at the forefront, promoting a digital transition shaped by European values.

More than 100 EU laws pertaining to digitalisation have been passed and 270 regulators are active in EU member states' digital networks. While these laws provide data security and privacy protections, they have also placed a notable strain on organisational budgets. A 2024 Veeam study into the implementation of the Network and Information Security Directive (NIS2) found that 68% of companies required additional budget to comply with the directive, while 95% diverted funds from elsewhere in the business to cover compliance costs. An analysis requested by the European Parliament in 2025 found that entrepreneurs and investors often cited regulatory fragmentation, due to an overlap of EU regulation and national certification schemes, as an impediment to European tech competitiveness.

Recent proposals such as the Digital Omnibus Regulation Proposal and the EU Cybersecurity Act proposal have sought to address these concerns. The Digital Omnibus, released in November 2025 and supported in the Berlin Declaration, would remove overlaps in regulation and streamline reporting by cutting 25% of existing EU compliance costs. The EU Cybersecurity Act proposal would streamline certification frameworks and introduce security provisions, such as the restriction and removal of high-risk suppliers from critical ICT functions within the EU. The EU has already created voluntary guidance to reduce the use of perceived high-risk suppliers like Chinese companies Huawei and ZTE through the 5G network-security 'toolbox'. The effectiveness of such voluntary measures was evident when in June 2025 the Spanish government signed – and then cancelled – a €10 million contract with Huawei to manage judicial wiretaps.

Strategic exposure through digital overdependency

The EU's digital dependency on the US and other non-EU technology providers is not a recent issue. A 2019 estimate stated that 92% of the Western world's data is stored in the US. In 2025, Proton found that more than 74% of Europe's publicly listed companies depend on US-based technology. The EuroStack project estimated that 80–90% of EU cloud computing is provided by three US hyperscalers – Amazon Web Services (AWS), Microsoft and Google. A 2025 study by Asterès concluded that European businesses spend €264 billion (1.5% of the EU's GDP) annually on cloud and software services from US providers. Finally, a 2025 survey found that 58% of European IT leaders cited integration with the US-dominated software stack as a major obstacle to digital sovereignty, with only 16% believing it could be achieved within the next five years.

The significant dependency on US providers challenges the feasibility of Europe's digital-sovereignty objective. However, during 2025, lawmakers in EU member states became increasingly unsettled by US foreign-policy decisions. Concerns over a US-held 'kill switch' on data flows were revived after the US briefly withheld intelligence from Ukraine. In addition, Microsoft was accused of locking International Criminal Court (ICC) officials out of their data to comply with a controversial US sanction against the ICC. While Microsoft and AWS have sought to reassure European nations by providing 'sovereign' cloud services, they have not been able to provide definitive guarantees that EU customer data would not be shared should the US invoke the CLOUD Act.

In response, efforts to reduce perceived vulnerabilities have intensified across Europe. In late 2025, Gartner found that 61% of Western European chief information officers (CIOs) want to increase the use of local or regional cloud providers. Lawmakers in the Netherlands, concerned by US-based Kyndryl's acquisition of local cloud-services provider Solvinity, called for government intervention to prevent the US company from accessing national ID systems. In January, the French government announced its decision to ban public officials from using US teleconferencing providers for government activities. In November, a group of lawmakers urged the European Parliament to enact a similar ban on US software in favour of local alternatives.

"When even old friends can turn into foes and their companies into a political tool, we cannot afford this level of dependence on foreign tech, let alone continue funneling billions of taxpayers' money abroad."

Letter to EU Parliament President Roberta Metsola from EU lawmakers, November 2025

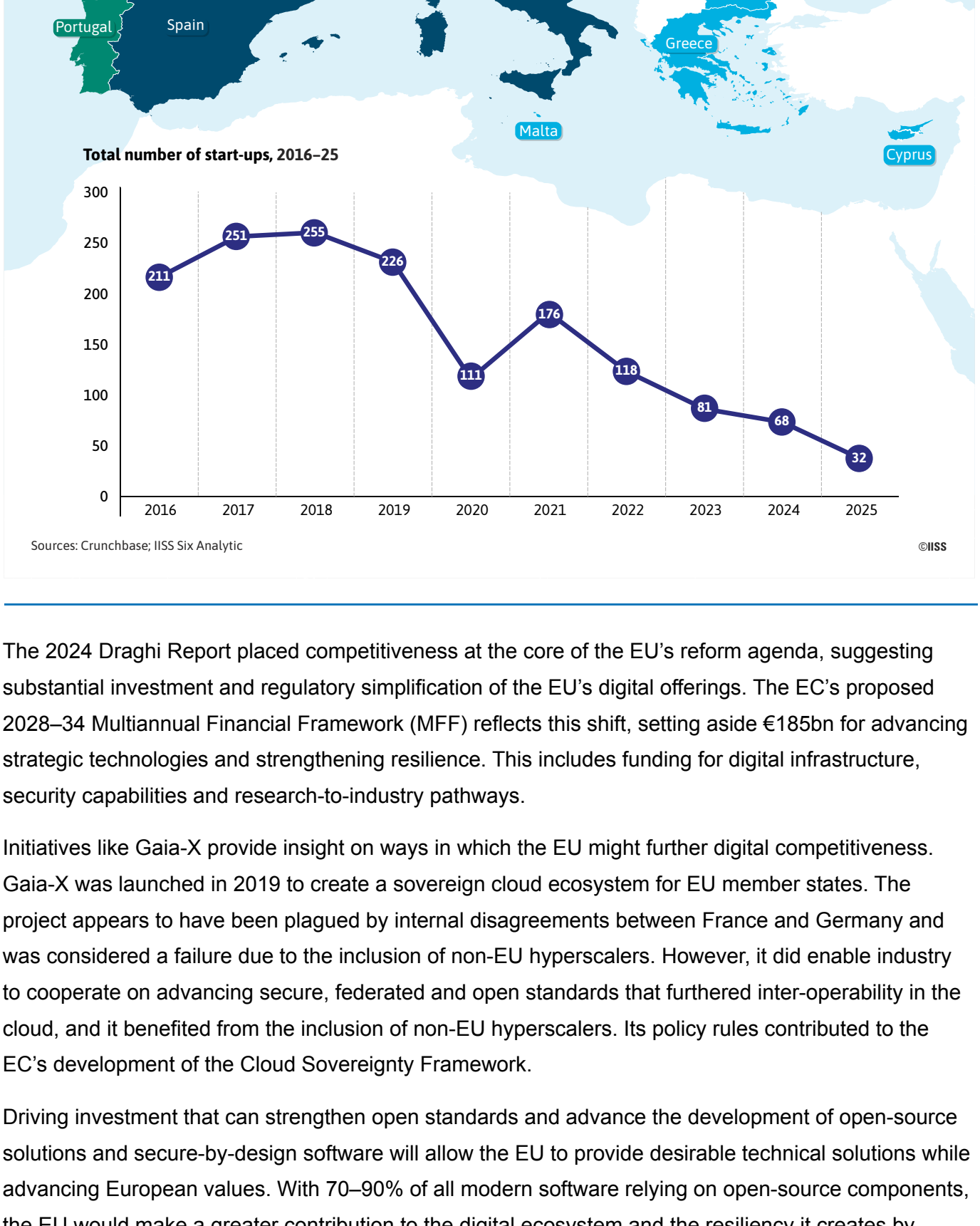
Furthering competitiveness and innovation

To increase digital sovereignty, EU institutions and member states need to address several structural challenges that constrain competitiveness and innovation. These include gaps in skills, capital and scale that limit the growth of EU digital firms; the complex patchwork of regulation that inhibits cross-border expansion and private investment; and a need to commercialise Europe's research strengths to advance innovation.

The EU's ability to compete is essential for the success of its digital-sovereignty strategy. It holds world-leading academic research institutes and talent, yet it has struggled to source and retain talent within digital industries. A report by the European Centre for the Development of Vocational Training in 2018 found that an estimated 55% of European employers found it difficult to fill ICT roles.

US capital has been instrumental for enabling European software start-ups to scale up and exit, with US technology providers funding the backbone of Europe's AI ventures. Successful European start-ups look to the US for acquisition, with US-based firms representing nearly 48% of the total transaction value of European technology mergers and acquisitions (M&A) deals in 2024, a substantial increase from 9% in 2015. The outflow of talent has weakened innovation within the EU, with suggestions that the lack of innovation centres contributes to this outflow.

Number of active cyber-security start-ups in Europe, 2016–25



The 2024 Draghi Report placed competitiveness at the core of the EU's reform agenda, suggesting substantial investment and regulatory simplification of the EU's digital offerings. The EC's proposed 2028–34 Multiannual Financial Framework (MFF) reflects this shift, setting aside €185bn for advancing strategic technologies and strengthening resilience. This includes funding for digital infrastructure, security capabilities and research-to-industry pathways.

Initiatives like Gaia-X provide insight on ways in which the EU might further digital competitiveness. Gaia-X was launched in 2019 to create a sovereign cloud ecosystem for EU member states. The project appears to have been plagued by internal disagreements between France and Germany and was considered a failure due to the inclusion of non-EU hyperscalers. However, it did enable industry to cooperate on advancing secure, federated and open standards that furthered inter-operability in the cloud, and it benefited from the inclusion of non-EU hyperscalers. Its policy rules contributed to the EC's development of the Cloud Sovereignty Framework.

Driving investment that can strengthen open standards and advance the development of open-source solutions and secure-by-design software will allow the EU to provide desirable technical solutions while advancing European values. With 70–90% of all modern software relying on open-source components, the EU would make a greater contribution to the digital ecosystem and the resiliency it creates by improving the auditability and portability of applications and data. The EC has dedicated €40m to the Open Internet Stack Initiative to create decentralised digital infrastructure.

"Europe is stepping up to accelerate the development of European innovation, to uphold strong data protection and to call for fair market conditions."

French President Emmanuel Macron on signing of the Berlin Declaration, November 2025

Conclusion

The EU is accelerating its digital-sovereignty agenda across multiple streams, but it requires time to develop and mature. The Berlin Declaration signalled that several EU member states are seeking to advance this process more quickly than EU institutions are able to deliver. Translating these ambitions into outcomes will require swifter political and regulatory coordination between EU institutions, member states and industry, a sustained and targeted investment at the EU and national level to advance digital capabilities, and a harmonisation of regulation that enables innovation.

Our Partners 2025

AIRBUS	Microsoft	Peregrine	Special Competitive Studies Project
Founding Partner	Founding Partner	Alliance Partner	Alliance Partner

eraneos	EDGE	SPEER GROUP
Alliance Partner	Official Partner	Venture Partner

CONTACT US

Hamburg Messe und Congress GmbH · Messeplatz 1 · 20357 Hamburg · Germany
Phone +49 40 3569-0 · Fax +49 40 3569-2203 · info@gsis-hamburg.com · www.gsis-hamburg.com

Follow us:

Management Board: Uwe Fischer (CEO), Heiko M. Stutzinger (CEO)
Hamburg Municipal Court, Reg. No. HRB 12 054
VAT No. DE811214125

Hamburg Messe + Congress