HORS-SÉRIE°3

CYBER-IT

MAGAZINE

CYBER IS A MARATHON NOT A SPRINT!

REGAINING CONTROL OF OUR DIGITAL DEPENDENCIES

In partnership with Plumber

Any questions? Please contact our team:
cyberit.magazine@gmail.com

EDITO

Europe’s digital landscape is at a historic crossroads, where every decision shapes our collective future. As non-European tech giants continue to extract hundreds of billions of euros from European businesses and public institutions, our data centers are now becoming vulnerable extensions of foreign ecosystems.

This special edition of the magazine, created for the Forum InCyber 2026, takes a clear look into the erosion of digital sovereignty.

In this issue, we will explore Europe’s growing dependence on foreign infrastructure. This reliance exposes sensitive, personal, industrial, and sovereign data to deep systemic risks, along with critical sectors such as healthcare, energy, and defense… Recent cases illustrate how a single decision made across the Atlantic can suddenly increase costs, disrupt vital services, or even threaten access to essential resources.

This issue goes even deeper. It explores the political and regulatory tools emerging to reverse the trend : dedicated observatories tracking strategic dependencies, the relocation of critical production, and a strategic shift in public procurement across Europe.

It also highlights key initiatives driving greater autonomy, including a federated and unified cloud project led by a broad alliance of European telecom operators, sovereign providers, innovative SMEs and open-source communities.

This special edition is a call to action. The time has come to regain control of our technological future and stop letting our most vital resources serve foreign powers.

Arnaud LEROY

CONTENT

Is Europe Losing Control to Big Tech?

The global digital market remains dominated by three American giants, which control nearly two-thirds of the market for infrastructure and platforms, while the rest of the industry struggles to keep up with the relentless speed of global growth...

General **Marc Watin-Augouard,** *founder of the InCyber Forum and former Inspector General of the French Armed Forces. He served as Director of the Research Center at the French National Gendarmerie Officers Academy until 2020.*

As we grow older, we all fear physical or mental dependence.

Relying on others for the simplest tasks, being at the mercy of their failures, feeling powerless in the face of minor difficulties, or becoming vulnerable to those who would take advantage of our inability to defend ourselves, these are fears shared by us all. Dependence means losing control over one's own future.

For institutions, businesses, public administrations, and the State, dependence is not a matter of old age. It is the result of a series of compromises, misplaced trust, and concessions that reduce freedom of action.

This shift is often almost invisible. Decisions are made by different actors, at different times, with a technical rather than strategic mindset. The wake-up call can be brutal, especially when the geopolitical landscape changes and yesterday's allies become tomorrow's threats.

Digital sovereignty is not about isolation or self-sufficiency.

Mutual dependence should guide political and economic decision-makers.

This demands a clear vision and strong leadership. But it also requires every decision to protect Europe's digital freedom to act.

Digital sovereignty is not built through declarations. It takes a series of deliberate choices, each of them seemingly small, but together they determine whether we remain in control of our digital future or quietly give it away.

The time for complaints, resignation, and fatalism is over. What matters now is the determination to take back control and rebuild our autonomy. This takes vision, leadership, and the will to act. And then, action.

Today's decision-makers carry a big responsibility. If these efforts fail, citizens risk becoming increasingly dependent on Big Tech, confined to the role of passive users in systems beyond their control. The InCyber Forum theme was no coincidence : it is a call for collective action.

To be, or cease to be, free in a cyberspace that consumes everything: that is the urgent question we must answer!

Général d'armée (2S)
Martin Watin-Augouard
Founder of the Forum InCyber

Digital Dependence
Economic Reality and Fragile Sovereignty

According to a 2025 study by Cigref (the French association of major public and private companies and organizations), European companies collectively spend **€265 billion each year** on digital tools and services controlled by non-European providers

According to a 2025 study by Cigref (the French association of major public and private companies and organizations), European companies collectively spend €265 billion each year on digital tools and services controlled by non-European providers

This significant amount, equivalent to the GDP of some European countries, does not simply pay for subscriptions or software licenses. It represents a major drain on Europe's capital, depriving Europe of the economic leverage it needs to build its own technology champions. However, this dependence goes far beyond financial concerns. It affects critical infrastructure, enterprise software, cloud platforms, and even the productivity tools used every day.

Companies such as Microsoft with Office 365 and Azure, Amazon Web Services, Google with Google Workspace and Google Cloud, and Salesforce dominate these markets, setting the standards and shaping the architecture of Europe's digital environment. In France, for example, more than 80% of large companies rely on American SaaS suites for email and collaboration, while

hyperscale public clouds providers now host 70% of critical deployments

European data centers are becoming extensions of the Silicon Valley, hosting data subject to the U.S Cloud Act and similar extraterritorial regulations.

The acquisition of VMware by Broadcom perfectly illustrates the risks of this type of dependence. Announced in 2023 and completed in 2024, the deal triggered major disruption for customers: sharp price increases up to 300% on some contracts, new contractual terms requiring forced annual commitments, and growing strategic uncertainty for European users.

Thousands of companies, including public administrations, found themselves trapped in a locked-in ecosystem, forced either to migrate to costly alternatives or renegotiate under pressure.

The consequences go far beyond procurement costs. They include the loss of control over sensitive personal, industrial, and sovereign data, exposed to foreign jurisdictions and the risk of forced transfers.

And European innovation also suffers. Trapped in closed ecosystems, startups and SMEs struggle to innovate without relying on roadmaps defined elsewhere, often in the United States. Faced with this growing outflow, pressure is building across Europe. Cigref, the association representing major French companies and public organizations, warns of a “systemic risk,” while Brussels moves forward with measures such as the Data Act, the AI Act, and the Digital Markets Act to enforce reciprocity and rebalance market dynamics.

The €265 billion spent each year risks becoming the largest unintended transfer of wealth to global tech giants at the expense of Europe’s digital revival.

The question is no longer whether the problem exists, but whether Europe is willing to act or accept long-term dependence

Reliance on non-European technologies became a structural vulnerability with far-reaching consequences for the continent.

Europe is now deeply tied to foreign tech giants, subject to their priorities with limited ability to respond. This dependence undermines the very foundations of sovereignty, turning tools meant to empower into invisible constraints.

Beyond the numbers: control over critical infrastructure

Decisions made by foreign governments or non-European companies can abruptly disrupt access to critical technologies. Extraterritorial laws such as the U.S. Cloud Act, along with export restrictions, illustrate how infrastructure can be used as a tool of political leverage.

A single decision in Washington can restrict access to essential services for European banks, hospitals, or defense systems. At the same time, U.S, China tensions threaten supply chains for semiconductors and software.

As a consumer, Europe bears the consequences of these power struggles without having a real say in the matter, leaving it exposed to ongoing technological pressure.

Sensitive data, whether personal, industrial, or governmental, continues to be processed and stored on foreign infrastructure, often outside Europe.

This creates exposure to economic espionage, mass surveillance, and potential misalignment with Europe’s data protection framework, including the GDPR, one of the strictest in the world

Despite record fines, data flows continue toward servers located in the United States or China, where they may fall within the reach of foreign intelligence agencies.

This web of dependencies is not inevitable. Initiatives such as Gaia-X and European Common Compute Power aim to lay the foundations for a European cloud, while a growing number of players are working to demonstrate that viable alternatives exist.

Without bold political will, strategic public procurement, major investment funds, and real consequences for vendor lock-in, Europe risks continuing to surrender its digital resources to foreign tech empires

HAUT-COMMISSARIAT
À LA STRATÉGIE
ET AU PLAN
Liberté
Égalité
Fraternité

Paths to Regaining Control

1 - The French digital sovereignty observatory

" Sovereignty starts with a clear understanding of our dependencies: which technologies we rely on, in which sectors, and for what purposes. That is the role of the Digital Sovereignty Observatory, which I have entrusted to the High Commission for Strategy and Planning »

Anne Le Hénanff
Minister for Artificial Intelligence and Digital Affairs

Amid this growing sense of urgency, France marked a turning point in January 2026 with the launch of the Digital Sovereignty Observatory.

But the announcement also invites scrutiny: why launch a new initiative when several existing structures are already working toward similar goals?

In 2014, the **Observatory for Digital Rights and Freedoms** was launched by a coalition of associations and trade unions, including the LDH, France's Human Rights League, and CECIL, a research group focused on citizenship, digital technologies, and civil liberties. Its mission was to defend fundamental rights against expanding surveillance mechanisms.

The following year, in 2015, **the Institute for Digital Sovereignty** was created to bring together economic players in the sector and put forward concrete proposals.

In 2017, a citizen-led movement led to the creation of the French Observatory for Digital Independence.

Then, in 2021, Télécom Paris and Netexplo launched their own **Technology & Digital Sovereignty Observatory**, with the support of Cédric O, then France's Secretary of State for Digital Affairs.

Launched at the beginning of the year, with a clear ambition to expand rapidly across Europe, the Observatory examines the factors that make us vulnerable. It looks at the geographic origin of hardware components, such as semiconductors, network equipment, and security hardware, as well as the structure of supply chains, identifying areas of concentration, including dependence on a limited number of countries or suppliers.

It also documents exposure to extraterritorial legal regimes by identifying technologies and services subject to foreign laws that may affect access to data or infrastructure.

On this basis, the Observatory produces summary indicators, dependency maps covering areas such as healthcare, energy, finance, and public administration, as well as technology-specific mappings to track how these dependencies evolve.

This work will feed into periodic reports, dashboards, and, in some cases, thematic alerts when a specific risk is identified, such as increased reliance on a single supplier.

Public authorities can use these findings to prioritize investment policies, target support programs for specific industrial segments, or adapt the regulatory framework.

These insights can also help large companies and operators of essential services assess their own exposure and guide their procurement strategies.

When several countries work together, the Observatory can take on a multinational role, for example at European level, by harmonizing measurement methodologies and making it easier to compare dependencies across Member States.

Led by the High Commission for Strategy and Planning and championed by Minister Anne Le Hénanff, this strategic initiative reflects a clear political ambition: to regain control over our digital future.

THREE PRIORITIES

1
Map critical dependencies through a shared assessment

2
Equip public and private buyers with decision-making tools

3
Help guide public policy on digital sovereignty

First findings and briefings are expected in spring 2026.

Paths to Regaining Control

2 - Bringing critical hardware production back to Europe?

" Europe is at a strategic crossroads in technology. Its heavy dependence on non-European players, from U.S. hyperscalers for cloud services to Asian foundries for semiconductors, has become both a major economic vulnerability and a real risk to its sovereignty »

In practical terms, this approach can be defined as follows: Relocating the production of strategic digital hardware means developing or strengthening industrial capabilities, within a given territory, in areas considered essential to the functioning of the digital economy.

This includes **semiconductors**, from chips and memory to more specialized components.

It also covers **network equipment**, routers, switches and antennas, **certain cybersecurity hardware**, such as hardware security modules and encryption devices, as well as the physical infrastructure that underpins **data centers**.

The goal is to increase the share of these components produced locally, or within trusted regions, in order to reduce exposure to external shocks.

In practice, this relocation effort relies on several types of measures.

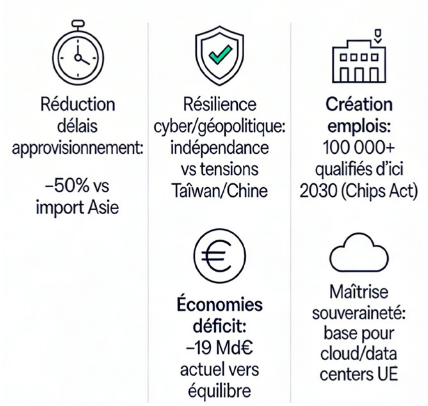
The first one is public support: investment grants, loan guarantees, tax credits for research and development, and co-financing programs with private partners.

These measures are often tied to formal commitments from industry players: **building factories** in specific countries, maintaining a minimum level of local production, transferring or retaining design and engineering expertise, and **creating skilled jobs.**

Cooperation frameworks can also be established between countries, or within regional blocs, to coordinate industrial sites, **avoid duplication, and distribute areas of specialization**.

Some countries, for example, may focus on wafer fabrication, while others specialize in packaging or testing.

A digital sovereignty perspective

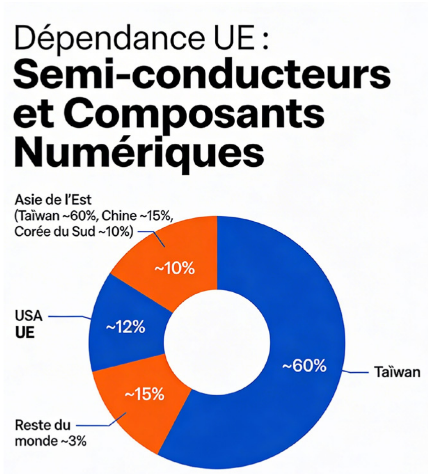


The objective is to anchor a significant share of the physical foundations of the digital economy within Europe: the hardware on which cloud services, critical information systems, communication networks, and cybersecurity infrastructure all depend.

The European Chips Act, for example, sets a target of doubling the European Union's share of global semiconductor production from 10% to 20% by 2030, backed by an estimated €43 billion in public funding to support the ecosystem.

Relocation also depends on the surrounding infrastructure: access to energy, transport networks, skilled labor, supplier ecosystems, and research centers. It is part of a long-term industrial policy approach. From an operational standpoint, developing these local capabilities helps reduce dependence on a limited number of countries or regions for key components.

It also gives Europe greater control over supply timelines and conditions, and more room to maneuver in the event of geopolitical tensions, export restrictions, or logistical disruptions.



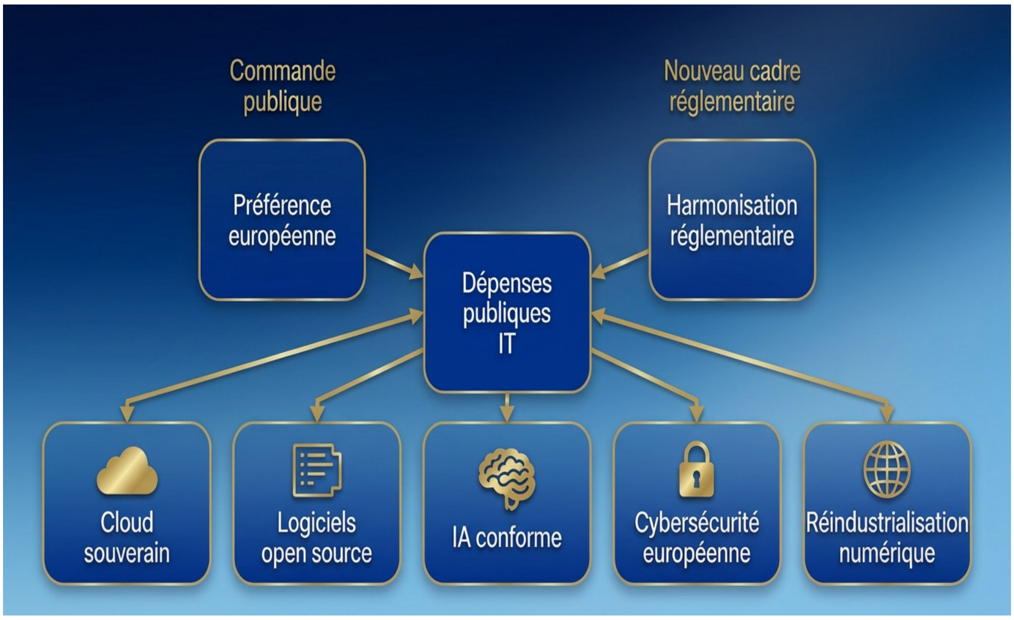
Paths to Regaining Control

3 - Public Procurement and a New Regulatory Framework

" Reforming digital public procurement would mean redirecting the €2 trillion spent each year by European public administrations toward sovereign solutions. A principle of EU preference would give an advantage to providers that guarantee data localization, local operational control, and the prioritized use of open source »

When supported by an appropriate regulatory framework, public procurement becomes one of the most powerful tools for steering Europe's digital market toward genuine technological sovereignty.

In other words, the billions of euros spent each year by public administrations could become a strategic tool for reindustrialization, provided they are directed more effectively. A clear and robust principle of European preference in digital procurement would allow public buyers to create lasting, predictable demand for European providers. This would apply across the public sector, from central government and local authorities to hospitals, universities, and essential operators such as energy providers and public banks.



Such a shift would directly benefit sovereign cloud providers, certified open-source software vendors, compliant AI platforms, and European cybersecurity solutions.

But this kind of structural change can only deliver results if it is backed by a clear, unified regulatory framework that reflects operational realities. Public authorities must work toward a coherent legal architecture, one that is both protective and practical, so that economic players can operate in a clear, predictable, and fair environment.

This requires strict and consistent harmonization of rules on data and metadata sovereignty, in order to provide legal certainty for cross-border exchanges and avoid divergent interpretations between national laws.

This harmonization should be paired with a pragmatic review of existing rules on AI, digital services, and data protection, including the AI Act, GDPR, and the DSA, so they support innovation without becoming a punitive burden.

The regulatory framework must also bring greater clarity to the certification requirements for critical digital infrastructure.

Such clarity is important to ensure a consistent level of security and compliance across the European Union, while avoiding duplication, conflicting requirements, and administrative burdens that slow innovation.

It would give European companies a more trusted environment in which to grow, lower barriers to public procurement, and make it easier for their solutions to qualify. A common framework would also provide a solid basis for the mutual recognition of certifications, making cross-border cooperation easier and helping create a truly integrated digital space.

By aligning these two tools over the long term, public procurement and regulation, European states could turn what has so far been a patchwork of scattered spending into a strategic engine for digital reindustrialization.

We see this as a way to build a unified digital space based on trust and transparency, with greater control over key technologies for all citizens and businesses.

EURO-3C, Europe's leading sovereign cloud project

The European Union has just launched EURO-3C, a strategic project backed by €7 million in funding under the Horizon Europe programme.

Announced at the Mobile World Congress 2026 in Barcelona, the consortium brings together 87 European organizations to build the continent's first large-scale federated Telco-Edge-Cloud infrastructure, reducing Europe's dependence on U.S. cloud providers.

This landmark project will demonstrate Europe's ability to deliver advanced digital services entirely through its own infrastructure.

Cloud computing has become the backbone of Europe's digital economy. Professional email, collaboration tools, artificial intelligence applications, document storage, data backup, and social media all rely on these distributed infrastructures.

Yet the vast majority of European cloud spending still flows to U.S. hyperscalers. Amazon Web Services, Microsoft Azure, and Google Cloud account for between 60% and 70% of the market. Their dominance rests on several advantages: vast financial resources, allowing them to invest heavily in global infrastructure, deeply integrated software ecosystems, rapid deployment capabilities that appeal to European businesses and the ability to bundle a wide range of services into a single environment.

The U.S. Cloud Act, enacted in 2018, allows American authorities to request access to data held by companies under U.S. jurisdiction, even when that data is stored on European servers. This legal reality has fueled a long-running debate over whether European organizations truly control their most critical data, particularly in sectors such as healthcare, defense, finance, and energy. EURO-3C aims to deploy more than 70 edge and cloud nodes across 13 European countries. Its architecture combines three complementary technologies: telecom networks, designed for 5G connectivity and future 6G readiness, edge computing, which brings processing power closer to end users and reduces latency.

Europe wants to build a federated cloud as the foundation for a sovereign, interoperable cloud infrastructure.

The physical location of data centers in Europe does not, on its own, guarantee data sovereignty

The EURO-3C consortium brings together a broad range of complementary players.

This multi-operator, multi-provider model is designed to ensure interoperability and prevent the emergence of national technology silos.

Established European providers such as OVHcloud, France's leading sovereign cloud provider, and IONOS, a major German cloud specialist, supply the physical infrastructure.

Specialized technology SMEs such as Scille, in cybersecurity, and Krateo, in platform engineering, bring agility and targeted expertise.

The consortium also includes key players in open source and sovereign cloud, including SUSE, a provider of Linux and Kubernetes solutions, and OpenNebula, which specializes in cloud orchestration.

By redirecting part of the €264 billion currently flowing each year to the United States, EURO-3C could help create hundreds of thousands of skilled jobs and fund European R&D.

The project aims to capture 15% to 20% of the sovereign cloud market by 2030, a realistic target if adoption among SMEs follows the path already taken by larger organizations.

The challenges remain significant : competitive pressure from well-established rivals, high initial migration costs, and the complexity of coordinating efforts across 13 countries.

With EURO-3C, Europe aims to move beyond the role of passive consumer and become the architect of its own digital future

A Bold Ambition with limited Funding...

EURO-3C is more of a pilot project than an industrial-scale deployment designed for the market. At this stage, it is not intended to create a large-scale cloud infrastructure.

Why? Competing with hyperscalers requires infrastructure at a scale usually measured in tens of billions of euros, an order of magnitude far beyond the announced €75 million budget.

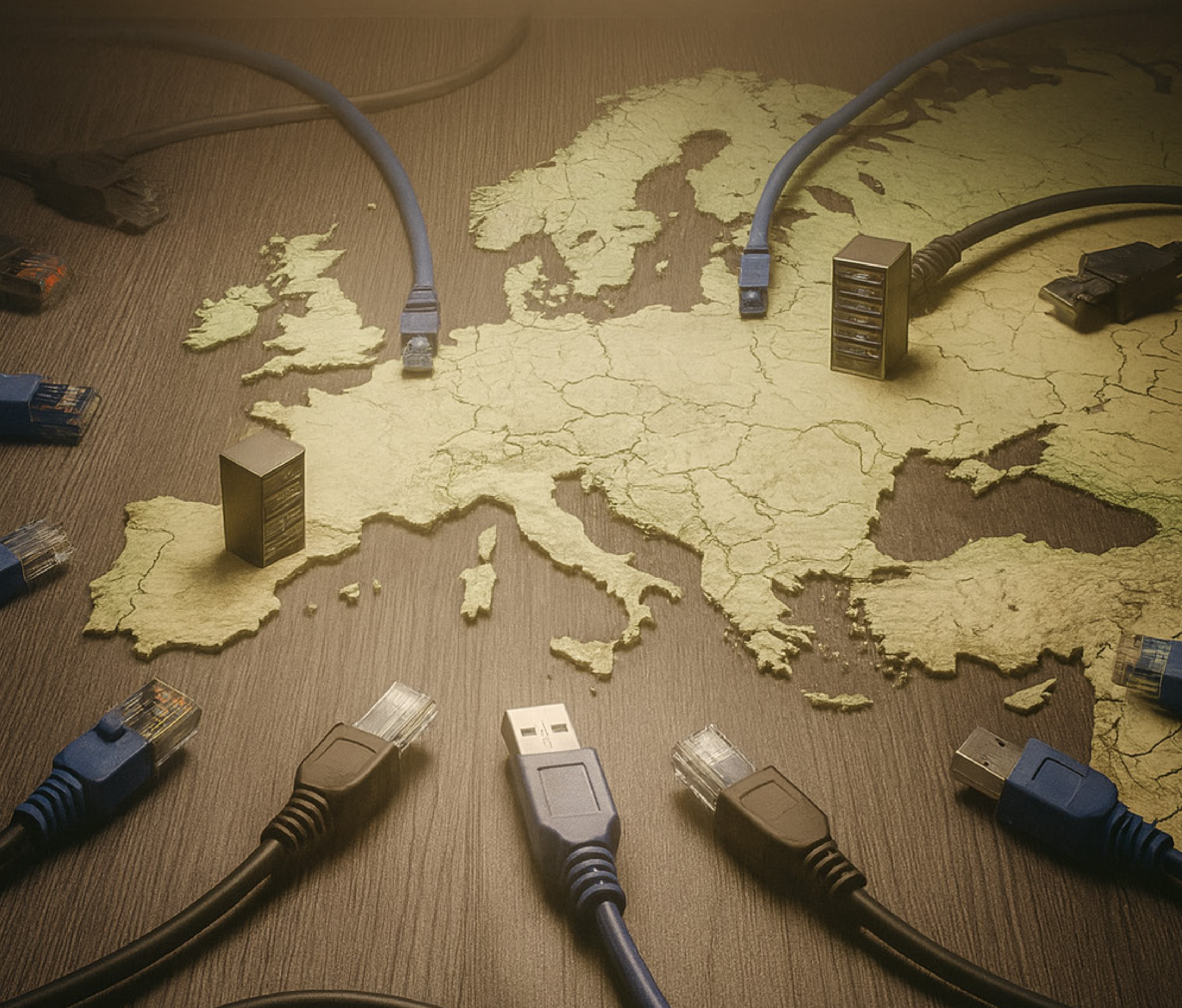
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR, DE LA RECHERCHE ET DE L'ESPACE
Liberté Égalité Fraternité

horizon europe

CREDITS

Editor-in-Chief : Arnaud LEROY
Graphic Design : Arnaud LEROY
English Translation : Maëva ASTORGA
Magazine's sponsor : Guillaume POUPARD

April 2026



IN CYBER FORUM
31 MARCH - 2 APRIL 2026
LILLE, FRANCE

In partnership with Plumber