ie UNIVERSITY
CENTER FOR THE GOVERNANCE OF CHANGE

FEBRUARY 2026

THE GEOPOLITICS OF THE DIGITAL REVOLUTION

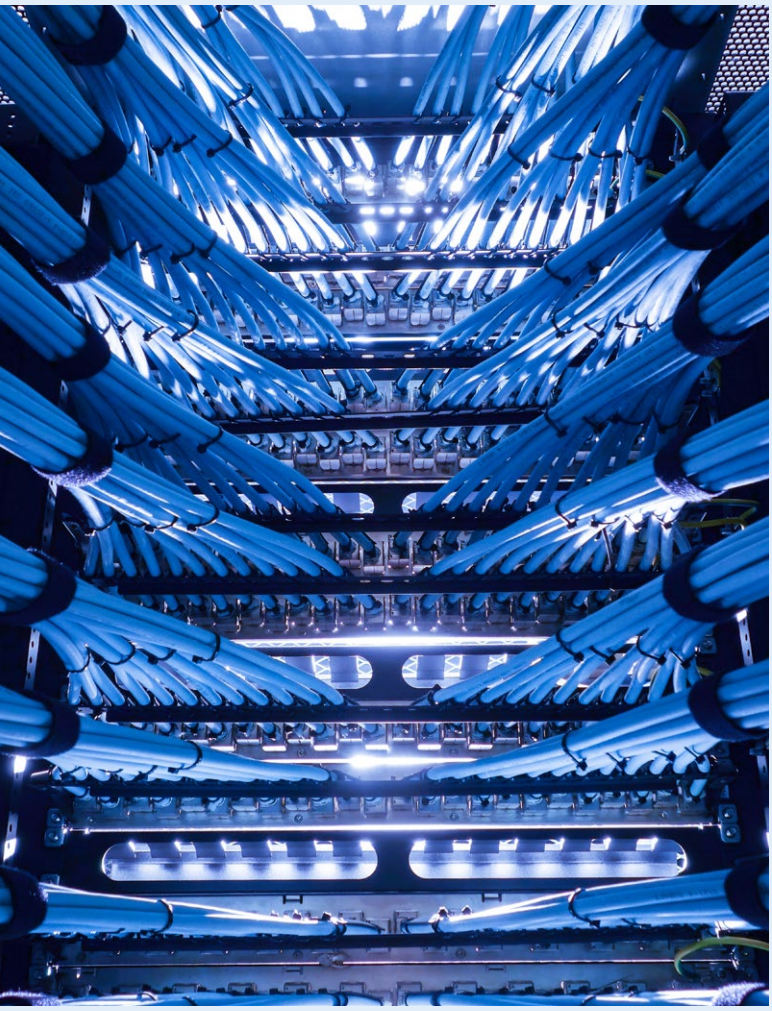
Europe's Defining Test

Miguel Otero Iglesias and Gonzalo Rodríguez Gordo

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The digital transformation has entered a new geopolitical phase. Digital technologies are no longer neutral enablers of economic modernization, but **foundational infrastructures** through which power is exercised, dependencies are created, and strategic influence is projected. Artificial intelligence, semiconductors, cloud infrastructures, data governance, and digital payment systems now constitute central arenas of geopolitical competition, shaping the ability of states and political communities to secure autonomy, resilience, and economic advantage.



This environment is increasingly confrontational. Major powers are consolidating **technological blocs** and leveraging control over critical supply chains and platforms as instruments of statecraft. Recent U.S. initiatives such as the Pax Silica agenda illustrate a push to structure AI development and supply chain security around preferred partners and excluded rivals. At the same time, China's rapid advances in AI and its expanding technological footprint underscore the accelerating nature of global technological rivalry. Regulatory divergence itself has become contested: enforcement actions by the European Union against dominant platforms have triggered political backlash abroad, highlighting that digital rule-setting is now inseparable from broader geopolitical tensions.

For the European Union, this shift marks a moment of strategic realization. Europe's digital model has been built primarily on regulatory power and the projection of democratic norms, rather than on ownership and control of the critical technological capabilities that structure the digital economy. The EU has shaped global debates through landmark frameworks such as the GDPR, the Digital Services Act, the Digital Markets Act, and the AI Act.

> Yet regulatory authority alone is increasingly insufficient in an international system where sovereignty is conditioned by material capabilities, technological scale, and infrastructural control.

Technological innovation generates significant strategic advantages, particularly in deep tech domains classified as high-risk where leadership is highly concentrated, dual-use military applications are possible, and other countries lack alternative supply chains or research capacity. Therefore, in crucial fields such as defense, leadership in **deep tech technologies may be translated into strategic superiority**. The current geopolitical context has thus started a global technological race in which major powers compete fiercely, triggering trade conflicts and eroding cooperation within international institutions.

This report argues that digital sovereignty has become indispensable for Europe and its citizens. Digital sovereignty does not imply technological autarky, but the capacity to make **autonomous decisions in the digital domain**, guided by European values and strategic priorities, while reducing exposure to coercion and structural dependency. The geopolitical context and the dynamics of the data-driven economy confront Europe with deep dilemmas:

- openness versus security,
- alliances versus autonomy,
- competitiveness versus social welfare,
- and value capture versus democratic safeguards.

Drawing on the analyses developed in this third work package of our multiannual project *The Digital Revolution* and the Social Contract, the report identifies four interconnected domains in which European action is urgently required, both internally and through partnerships with like-minded actors:

01/

Reinforcing regulatory capacity and norm-setting power through stronger institutional coordination, credible enforcement, and coalition-building with partners across the Global North and South (see the recent agreements with Mercosur and India), including via initiatives such as the Global Gateway.

03/

Capturing the benefits of the Generative AI + data-driven economy by enabling European firms to innovate, scale, promoting strategic catch-up to overcome legacy vulnerabilities, and reconceptualizing data as a strategic asset underpinning innovation and competitiveness through hardware and software.

02/

Building control over key layers of the technology stack by supporting European competitors in strategic infrastructures such as cloud, compute, AI deployment, and semiconductors through innovation ecosystems, while diversifying dependencies and reducing exposure to external chokepoints.

04/

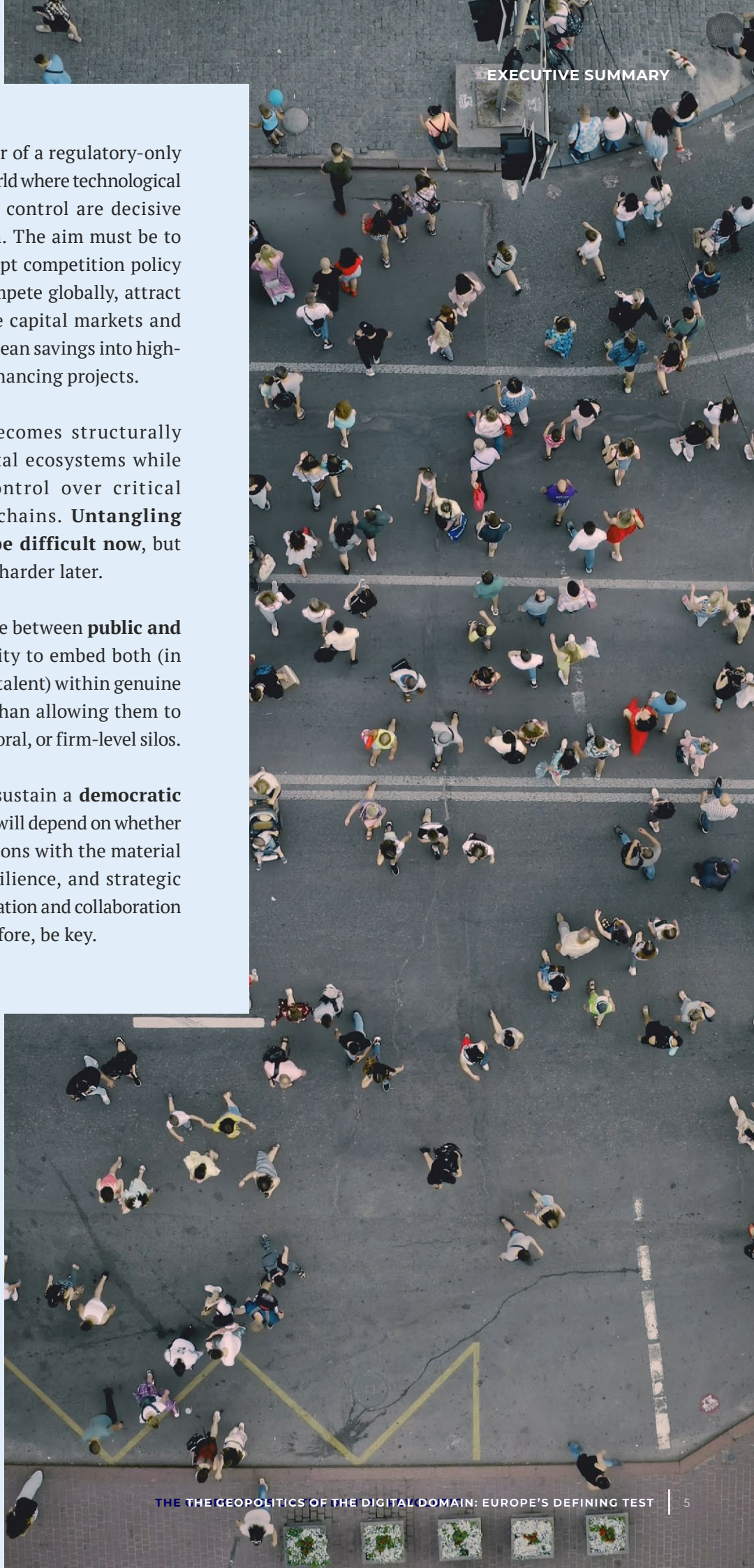
Enhancing the resilience and adaptability of critical infrastructures, particularly in the monetary and financial domain, through the development of European safe assets, payment systems, deeper and more integrated capital markets, a stronger international role for the euro, and the adoption of the technology and capabilities embedded in the new forms of money (CBDCs & Stablecoins).

The stakes are high. The power of a regulatory-only European model is waning in a world where technological leadership and infrastructural control are decisive sources of geopolitical strength. The aim must be to integrate the single market, adapt competition policy to enable European firms to compete globally, attract human talent and complete the capital markets and banking unions to channel European savings into high-risk, high-tech, productivity-enhancing projects.

At risk is whether Europe becomes structurally subordinated to external digital ecosystems while remaining vulnerable to control over critical chokepoints in global value chains. **Untangling Europe's dependencies will be difficult now**, but delaying action will make it far harder later.

Europe's challenge is not a choice between **public and private initiative**, but the ability to embed both (in terms of strategy, resources and talent) within genuine European architectures rather than allowing them to remain confined to national, sectoral, or firm-level silos.

Ultimately, Europe's ability to sustain a **democratic social contract** in the digital age will depend on whether it can align its normative ambitions with the material foundations of sovereignty, resilience, and strategic agency. Public and private cooperation and collaboration in the same direction will, therefore, be key.



1. INTRODUCTION

The digital transformation has become one of the defining forces reshaping the international system. Once treated primarily as a driver of economic modernization and social connectivity, digital technologies are now increasingly understood as a core domain of geopolitical competition.

> Data, artificial intelligence, semiconductors, cloud infrastructures, and digital payment systems have become strategic assets that structure global power relations, expose vulnerabilities, and create new forms of dependency and coercion.

This shift is unfolding in an increasingly confrontational environment. The global race for technological leadership is no longer framed only in terms of innovation or economic advantage, but in terms of strategic alignment and geopolitical hierarchy. Recent U.S. initiatives such as the **Pax Silica** agenda, presented as a flagship effort on AI and supply chain security, illustrate how Washington is seeking to consolidate an inner circle of countries at the leading edge of AI development and financing, while keeping other actors dependent or excluded from critical technological ecosystems. At the same time, China's rapid advances in artificial intelligence, symbolized by the arrival of new large-scale models such as DeepSeek, have reinforced perceptions of an accelerating AI race in which global leadership is increasingly contested.

As the international order gradually shifts toward a more fragmented and multipolar configuration, digitalization is profoundly altering the foundations of economic statecraft and sovereignty. Classical concepts in international political economy such as (inter)dependence, production, security, technological autonomy, and strategic influence require renewed interpretation in a world where control over digital infrastructures and technological standards increasingly determines states' room for maneuver.

The digital domain has also become a site of regulatory conflict. Competing governance regimes are diverging sharply, and the legitimacy of different regulatory approaches is increasingly questioned. The European Union has emerged as a global leader in rights-based digital regulation, advancing frameworks such as the **GDPR**, the **Digital Services Act (DSA)**, **the Digital Markets Act (DMA)**, and the **AI Act**. Yet enforcement actions against major U.S.-based platforms have triggered political backlash, with prominent American voices framing European regulation as an illegitimate constraint on U.S. innovation and corporate power. The European Commission's investigations into platform practices, including recommender systems under the DSA, highlight how digital rule-setting is now inseparable from broader geopolitical tensions among allies.

Under external pressure and intensifying strategic rivalry, Europe's own approach is also evolving. Recent initiatives such as the **Digital Omnibus proposal**, which introduces more flexibility in implementation timelines and risk-classification requirements, suggest a recalibration of regulatory ambition in response to competitiveness concerns. Simultaneously, the EU is placing greater emphasis on capability development through industrial and infrastructural initiatives such as the **AI Continent Action Plan** and proposals for large-scale "gigafactories." Regardless of their eventual success, these efforts signal a shift: Europe increasingly recognizes that sovereignty in the digital era cannot rest on regulation alone but requires material capacity and technological depth.

These developments are unfolding alongside a broader reconfiguration of alliances. Digital interdependence is straining established partnerships, and geopolitical rhetoric has sharpened even within the transatlantic relationship. Recent debates surrounding U.S. strategic priorities, including high-profile statements at the Munich Security Conference and renewed emphasis on security-driven technological blocs, underscore the degree to which Europe faces a more uncertain external environment. The digital revolution is thus accelerating not only technological change, but also strategic realignment.

Against this backdrop, the concept of digital sovereignty has moved to the center of European policy debates. Digital sovereignty refers not to technological autarky, but to the capacity of a political community to make autonomous decisions in the digital domain, guided by its own values, interests, and strategic priorities. It encompasses regulatory authority, control over key technological building blocks, resilience of critical infrastructures, and the ability to capture economic benefits from data and AI rather than allowing them to be extracted externally.

This report, produced under the Center for the Governance of Change's multiannual research program "The Digital Revolution and the New Social Contract", examines how digital transformation is reshaping geopolitics and how Europe can respond to the resulting strategic dilemmas. Drawing on the analyses developed in the third work package, it explores the competition between digital governance regimes (Schneider), the material foundations of digital power embedded in the technology stack (Ferreira Gomes et al), the evolving dynamics of the data-driven economy (Ciuriak), and the growing importance of monetary sovereignty in an era of digital finance (Otero et al).

Ultimately, the report argues that Europe's digital future is inseparable from its geopolitical agency. The challenge is not only to regulate the digital environment, but also to ensure that the European social contract can be sustained in a world where digital infrastructures and capabilities have become instruments of power, competition, and strategic dependency.

CONCEPTS, POLICIES AND REGIMES

02

2. CONCEPTS, POLICIES AND REGIMES

As the international system gradually reorients toward a multipolar configuration, the dynamics of global power are undergoing a marked transformation due, in part, to the extraordinary reach of the digital transformation, giving rise to dilemmas of sovereignty, geopolitics and geoeconomics.

From an economic perspective, especially since the Chinese government introduced the concept in its policy analysis in late 2019 and early 2020[1], data have features that make them historically unique. They can be considered as the **fifth factor of production**, alongside labor, land, capital and entrepreneurship, and they have a *quantum* characteristic, the same data asset is often "multi-status" (akin to "superposed" in quantum physics) and "multi-purpose" (akin to entangled)[2]. From a geopolitical perspective, digital technology has emerged as a highly contested domain among global powers. The race to dominate digital technologies, which have become the backbone of modern societies, carries direct implications for sovereignty.

> Thus, digitalization is profoundly reshaping the core dimensions of economic statecraft, making many of the classical concepts of political theory, international relations and political economy—sovereignty, independence, production, finance, technology autonomy and security—require renewed interpretation.

In this transformed landscape, academic communities and high-level policy actors are increasingly turning to concepts such as digital sovereignty, digital regimes, strategic autonomy, the tech race and the weaponization of critical infrastructures and systems to make sense of how power operates in the digital age.

2.1. DIGITAL SOVEREIGNTY FRAMEWORK

Digital sovereignty remains a fluid notion without a commonly agreed definition. Despite earlier presence in academic circles, the concept gained prominence in European policy debates during the Covid-19 pandemic, as dependencies in the European economy were newly perceived as critical vulnerabilities.[3] Some authors have linked this notion not only to purely technological aspects, but also to the economic, social, democratic, and even security aspects of the digital ecosystem.[4] In the European case, such ambiguity may be considered as an intentional feature of the concept in order to garner support across EU institutions, Member States, the private sector and other stakeholders whose interests differ.[5]

In practical terms, digital sovereignty can be described as the capacity of a political community to make independent decisions in the digital domain, guided by its own values, interests and strategic priorities. It requires control over key digital infrastructures to prevent external actors—whether foreign governments or dominant corporations— from unilaterally shaping, constraining, or weaponizing the digital environment on which societies depend. More concretely, digital sovereignty includes, among other objectives, reducing exposure to semiconductor supply restrictions imposed by third countries, securing the capacity to leverage the data generated by citizens for the development of applications and algorithms through the control of critical digital infrastructure and maintaining the ability to enforce lawfully adopted legislation without the threat of retaliation.

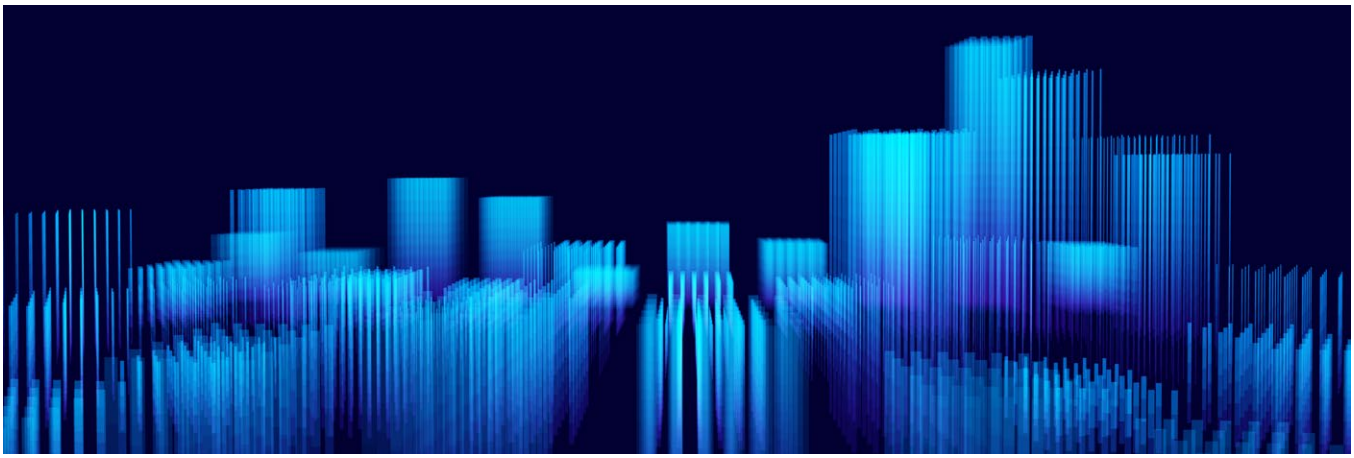
In its full scope, digital sovereignty is a broad and layered concept. Yet within its complexity, our research identifies four pillars that consistently define its core architecture across the policy papers included in the work package:

1. **Regulatory capacity and norm-setting power:** The ability to define, enforce and project democratic digital norms at home and abroad.
2. **Control of the technology layers (digital building blocks):** Fostering innovation, access to and control over the resources, chips, cloud infrastructures, data and applications (hard and software) that underpin the digital economy.
3. **Adaptability and modernization of critical digital infrastructures:** Ensuring that critical infrastructures remain resilient and adaptable to technological change. This includes the monetary domain, where Central Bank Digital Currencies (CBDC) and other digital assets (Stablecoins) exemplify how infrastructure modernization becomes a priority for sovereignty.
4. **The capacity to capture benefits from the digital economy:** The ability to appropriate economic rents from data, AI and digital infrastructures, rather than allowing them to be extracted externally.

> Given the intricate international connections and interdependencies present in the digital economy and its many layers, digital sovereignty depends not only on internal capabilities but also on the external strategic environment in which these capabilities are developed and deployed.

The struggle for technological and geopolitical dominance is prompting both established powers and emerging challengers to adopt a more assertive stance in defending—or attempting to reshape—the existing order. As a result, the competition between **digital governance regimes**—exemplified by the United States' (US) market-driven model dominated by big tech, China's state-centric approach, and a rights-based regulatory framework championed by the European Union (EU) and several like-minded middle powers—has become a central arena in which power is exercised.

Geopolitical competition is increasingly influencing sovereignty due to the concentration of key digital power resources —data, cloud infrastructures, semiconductors, AI systems and standards— in the hands of a small number of prominent actors. These asymmetries generate vulnerabilities and expose states and political communities to coercive pressures, limiting their ability to shape their digital environments and develop their own industrial and technological capabilities according to sovereign decisions.



For Europe, the geopolitical shock triggered by Russia's war of aggression against Ukraine in February 2022 reinforced the centrality of power politics and elevated the importance of the concept of **open strategic autonomy**. Although the term strategic autonomy had already been widely used during the first Trump administration, its meaning had largely been associated with security and with reducing excessive dependence on the North Atlantic Treaty Organization (NATO). More recently, however, open strategic autonomy has come to refer to the EU's capacity to act autonomously across strategically important domains—from defense and the economy to technology governance and the protection of democratic values.[6]

This broader understanding of open strategic autonomy reveals that European sovereignty is exposed in a wider range of domains than previously assumed, particularly as a result of shifts in the digital landscape. The monetary and financial system is a clear example: monetary sovereignty is increasingly entangled with the digital domain due to the rise of cryptocurrencies, stablecoins, new payment infrastructures and central bank digital currencies (CBDC), which are reshaping how monetary power is exercised.

> Technological innovation can translate into significant strategic advantages, particularly in deep tech domains classified as high-risk where leadership is highly concentrated, dual-use military applications are possible, and other countries lack alternative supply chains or research capacity.[7]

In contexts such as defense, leadership in deep tech technologies may be translated into strategic superiority.[8] Therefore, these conditions give rise to a global **technological race** in which major powers compete fiercely, triggering trade conflicts and eroding cooperation within international institutions.

2.2. THE MATERIAL FOUNDATIONS OF DIGITAL POWER: THE TECH STACK

If digital sovereignty describes the capacity to act autonomously in the digital domain, that capacity ultimately rests on a very concrete set of material foundations. Beneath data flows, platforms and algorithms lies a dense architecture of physical and virtual components that enables digital systems to function at scale. This layered architecture is often described as the technology stack, or tech stack: the interdependent set of resources, infrastructures, networks, software and data that together make digital services possible.

In the literature informing this report, the term "**tech stack"** refers to the way in which power is embedded in technology. The paper *Beyond LEGO—the Need for EU-based Building Blocks of Technology*, illustrates how seemingly intangible services, such as an AI chatbot, are in fact dependent on a chain of "digital building blocks" that span multiple layers: from critical raw materials, energy and water, to specialized chips, data centers and cloud infrastructure, to software frameworks, applications and user interfaces.[9] At each step, control over one layer conditions what is possible in the others, creating dependencies that are technical, economic and ultimately geopolitical. In this sense, the **EuroStack initiative**[10] is a comprehensive plan for digital sovereignty. It describes an "infrastructural layered framework for digital sovereignty" in which raw materials, semiconductors, networks, cloud computing, software, data and AI, cybersecurity, defense and even financial infrastructures form an integrated system rather than function as isolated sectors.

From this perspective, the concentration of market power in a few non-European actors across key layers translates into structural dependencies that constrain Europe's room for maneuver across the whole stack. An outsourced stack exposes the Union to potential supply disruptions in hardware, the weaponization of cloud and platform access, and the gradual erosion of its capacity to capture value and project its own normative preferences in the digital sphere.

The **European Competitiveness Report** by Mario Draghi[11] places a significant emphasis on the state of Europe's technological base as a central component of its diagnosis. It portrays a continent whose digital stack remains incomplete and reliant on external actors, and whose firms often struggle to turn scientific strengths into scaled industrial capabilities. The report argues that in order to reverse this trajectory, Europe must mobilize on the order of €750–800 billion in additional investment each year until 2030. This investment would allow to modernize infrastructure, deploy clean and digital technologies and rebuild strategic value chains. This effort should be accompanied by reforms that further integrate the single market, adapt competition policy to enable European firms to compete globally, and complete the capital markets and banking unions to channel European savings into high-risk, high-tech, productivity-enhancing projects.

That diagnosis has since been translated into a strategic roadmap by the European Commission: **its Competitiveness Compass**[12]. According to this roadmap, competitiveness is a condition for Europe's capacity to act in a world increasingly shaped by technological rivalry. The Compass argues that Europe must close its innovation gap, steer the green transition in ways that strengthen rather than weaken its industrial base, and reduce the dependencies that expose the Union to external shocks by developing capabilities and diversifying its alliances. It calls for accelerating investment in future technologies, deepening and simplifying the single market to allow firms to scale, and reinforcing the industrial ecosystems that can sustain next-generation technological capabilities. The underlying message for digital technologies is clear:

> Europe's tech stack will not become a source of strength unless the continent can build, host and deploy critical technologies at a scale that matches its ambitions.

Together, the European Competitiveness Report and the Competitiveness Compass present a comprehensive diagnosis of Europe's structural weaknesses and the outline of a collective response. They demonstrate that the state of the European digital, and more broadly tech stack is pivotal in determining whether the Union can align its market-shaping ambitions via regulation with a world where power increasingly depends on control over key technologies. Reconciling this regulatory vocation with the need to build and host critical capabilities at scale is emerging as one of the defining tests for Europe in the digital era. Unfortunately, so far only roughly 10% of Draghi's plan has implemented. Implementation to date remains limited relative to the scale of the challenge identified in Draghi's diagnosis.

On the other hand, the current data-driven economy is characterized by the rapidly growing deployment of **machine knowledge capital**. This form of capital substitutes for skilled labor while requiring massive investments in computation, energy resources, and advanced data centers and AI infrastructure. These features perpetuate the structural advantages of the U.S. and China, reflecting the scale dynamics of AI: the larger the data pool, the more powerful and valuable the resulting models become.

2.3. THE NORMATIVE FOUNDATIONS: COMPETING MODELS OF DIGITAL REGIMES

Digital governance regimes refer to the policies, regulations, and institutional frameworks that shape how digital technologies and the internet are developed, governed, and deployed. Across this landscape, **three competing models** have crystallized in the last decades around the U.S., China, and the EU, each structuring key domains such as data governance, security, innovation, and competition in distinct ways.[13] However, it must be noted that traditional approaches are changing with the volatility of the current geopolitical context.

The U.S. and China both prioritize speed and scale in technological innovation, yet they follow fundamentally different institutional trajectories. The U.S. model is anchored in market-driven dynamism, with limited ex ante constraints and a reliance on competition and private initiative to drive technological development. China's model, by contrast, is characterized by state-led control, where technological upgrading is closely aligned with political stability, economic planning, and national power.

The EU stands in contrast through a third approach, centered on *ex ante* regulation, strong protections for fundamental rights, and a public-interest orientation in the design of digital infrastructures, data spaces, and artificial intelligence (AI) systems.

Table 1: Digital Governance Regimes: US, China, and the EU (Adapted from Schneider (2025))

KEY DIMENSION	UNITED STATES	CHINA	EUROPEAN UNION
Regulatory Approach	Minimal regulation and a largely hands-off approach, with limited government interference to foster tech industry growth.	State-controlled regulation with strong oversight to ensure alignment with national priorities.	Strong regulatory framework emphasizing transparency, fairness, and accountability in the digital economy.
Innovation Focus	Prioritizes maintaining technological leadership, often placing innovation ahead of regulation.	Technology is treated as a tool for economic growth under close state supervision.	Promotes ethical and human-centric innovation, ensuring AI and digital technologies are safe, sustainable, and trustworthy.
Market Dynamics	Relies on market forces to address imbalances, avoiding heavy ex ante regulation unless necessary.	Government intervention plays a key role in steering markets and aligning firms with state objectives.	Seeks balance between regulation and competition, preventing monopolies while fostering competitive markets.
Economic Development	Market-driven model in which private technology companies lead innovation and global expansion. CBDCS not a priority Stablecoins private solution leader.	Government-driven technology sector supporting national economic strategies and long-term planning. CBDC already issued.	Digital development aligned with European values, emphasizing sustainability and social responsibility. Mixed approach: CBDCS + private solutions
Social Control	Limited direct state control over platforms, though concerns over misinformation and accountability are rising.	Technology is used as an instrument of social and political control, reinforcing digital authoritarianism through surveillance.	Emphasizes digital rights and democratic oversight, ensuring users retain control over data and online interactions.
Data Governance	Decentralized governance with private firms playing a dominant role; comprehensive privacy regulation remains limited.	Mass data collection and centralized state control of citizen data to ensure security and stability.	Comprehensive governance framework (notably GDPR) enhancing privacy, security, and user empowerment.
Global Influence	Global dominance driven by private firms (e.g., Google, Apple, Microsoft) rather than state-led strategies.	Exports its governance model through the Digital Silk Road, promoting infrastructure and standards abroad.	Projects regulatory standards globally through the "Brussels Effect," shaping governance beyond EU borders.

UNITED STATES: MARKET-DRIVEN MODEL

The U.S. digital governance regime is traditionally rooted in a liberal market philosophy that prioritizes economic freedom and private initiative. Regulators have historically granted technology companies wide latitude to innovate, relying primarily on *ex post* intervention in cases of clear harm or market failure.[14] This approach has translated into persistent federal-level gaps in areas such as privacy, content moderation, and platform regulation, including the absence of a comprehensive data protection framework and the continued scope of Section 230 of the Communications Decency Act of 1996, which limits platform liability for third-party content.

> This regulatory environment has enabled an unparalleled concentration of economic and technological power among major digital platforms, inspiring the notion of technofeudalism.[15]

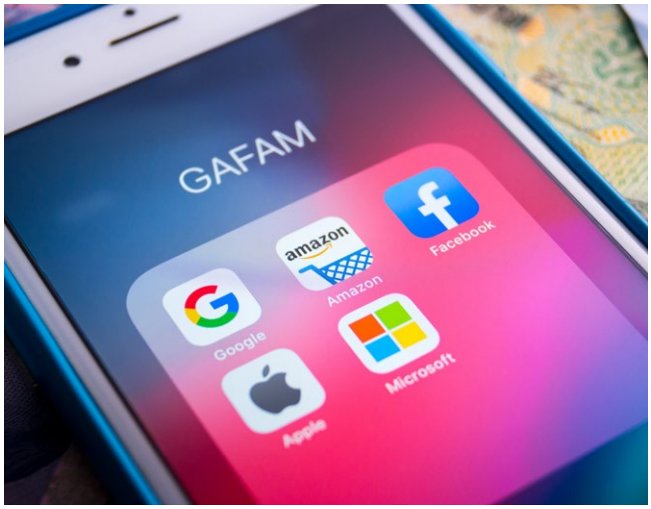
Firms commonly grouped under the acronym GAFAM—Google (Alphabet), Apple, Meta, Amazon, and Microsoft—dominate key segments of the global digital economy, accounting for over 90 percent of the market capitalization of the world's largest digital platforms and more than 94 percent of global funding for AI startups.[16] This dominance reflects a governance regime that has historically prioritized market-driven innovation over comprehensive digital regulation.

Recent administrations have introduced elements of adjustment without fundamentally altering this model. Under the Biden administration, increased oversight emerged through antitrust enforcement by the Federal Trade Commission and the Department of Justice, alongside an executive order on AI. However, these initiatives have operated within structural constraints that limit the scope of large-scale regulatory reform. Under the Trump administration, the model has further converged with corporate interests: Trump's second term is marked by a notably close relationship between the CEOs of major technology corporations—the growing informal political influence of major technology executives— and the presidency, amplifying the informal political influence of high-profile executives such as Elon Musk.

At the same time, industrial policy has re-entered the U.S. policy toolkit in response to intensifying geopolitical competition with China. The **CHIPS and Science Act** exemplify this shift, channeling tens of billions of dollars into domestic semiconductor manufacturing and advanced research. Rather than signaling a departure from the liberal market tradition, these measures represent targeted interventions justified by national security concerns and the objective of maintaining technological leadership.

This combination—market dynamism, selective security-driven intervention, limited ex ante regulation, and growing corporate influence—generates a powerful innovation engine, but it also produces structural tensions with international partners. These tensions stem not only from regulatory divergence, but from how the U.S. exercises external power to defend its own interests, including vis-à-vis close allies.

This dynamic has become visible in episodes where U.S. authorities have explicitly challenged EU digital regulation—such as criticism directed at the enforcement of the Digital Services Act (DSA) and the Digital Markets Act (DMA)—framing allied regulatory action against US-based platforms as illegitimate. As a result, disagreements over platform governance increasingly translate into broader geopolitical frictions, with concrete implications for the capacity of allied democracies to define and enforce rules governing their digital public spheres.



CHINA: STATE-CENTRIC APPROACH

Although there was a phase of extreme competition and laissez faire policies to generate technological muscle, China's digital governance model is fundamentally top-down, predicated on the belief that state intervention and oversight are essential for maintaining stability and preserving the authority of the Chinese Communist Party (CCP). The government has shielded its technology sector from foreign competition, directed competition to particular sectors and nurtured domestic champions through subsidies, tax incentives, and protective regulation, creating an environment designed to advance technological self-sufficiency across strategic domains. This model combines rapid digital modernization with extensive mechanisms of control—exemplified by the Great Firewall—while enabling firms such as Baidu, Alibaba, and Tencent to expand under close state supervision.

A major turning point occurred with the launch of **China's national AI strategy** in 2017, which marked the beginning of a more systematic regulatory approach to data, algorithms, and online behavior. By 2020, when it was acknowledged that data are a new factor of production, the CCP's "Common Prosperity" campaign provided the political justification for a far-reaching crackdown on private technology firms, including high-profile interventions targeting Ant Group, Alibaba, and Tencent. Regulatory instruments such as the **Cybersecurity Law, the Data Security Law, and the Algorithmic Recommendation Management Provisions** (2022) institutionalize this approach by requiring companies to align algorithmic outputs with Party-defined values and to grant authorities extensive access to data.[17] The state further consolidates influence through mixed-ownership structures, acquiring equity stakes in private firms and placing CCP members on corporate boards to ensure alignment with national priorities.

> Telecommunications and network equipment supplied by Huawei and ZTE, alongside smart-city and surveillance systems, offer partner countries relatively low-cost pathways to digitalization, but often generate long-term dependencies, including high debt burdens and repayment arrangements tied to strategic raw materials and infrastructure ownership.

Under its open access model, which is penetrating the so-called Global South, Beijing promotes data localization and sovereign control over information flows as attractive options for governments seeking greater autonomy from Western platforms, thereby diffusing legal and technical practices aligned with its own governance model[18]. Despite its authoritarian features, this model continues to rely on market-driven competition and innovation domestically, illustrating that rapid technological upgrading can coexist with far-reaching state control to the point that some believe that China is overtaking the U.S. in the AI race[19].

UE: RIGHTS-BASED, REGULATION-DRIVEN FRAMEWORK

Europe pursues a "third way" model of digital governance that places fundamental rights, democratic oversight, and the rule of law at the center of its digital policy. This approach contrasts with the regulatory shortcomings associated with the more market-driven U.S. model and with the state-centered techno-authoritarianism characterizing China's digital governance. The EU framework is oriented toward advancing public interest, rebalancing corporate power, and safeguarding democratic values.

> This model is operationalized through a growing and increasingly comprehensive body of legislation that reshapes how data, platforms, and digital services are governed. Within this framework, the EU's digital governance model rests on a layered regulatory architecture that serves distinct but complementary functions.

Foundational instruments such as the **GDPR**, the **DSA**, and the **DMA** establish core principles, rights, and obligations aimed at protecting individuals, rebalancing platform power, and ensuring fair competition. Alongside these, enabling and infrastructural measures—including the **Data Governance Act, the Data Act,** and the **Open Data Directive**—seek to organize the circulation, reuse, and accessibility of data in ways that support innovation while remaining consistent with public-interest objectives. A third set of instruments, oriented toward security and systemic risk management, such as **NIS2**, the **Cyber Resilience Act**, and the risk-based provisions of the **AI Act**, reflects a growing emphasis on resilience, cybersecurity, and the mitigation of vulnerabilities across critical digital infrastructures.

Box 1: Core EU Digital Governance Instruments

>FOUNDATIONAL

- **General Data Protection Regulation (GDPR):** Establishes strong rights for individuals over their personal data and strict obligations for controllers and processors.
- **Digital Services Act (DSA):** Harmonises rules for intermediary services and introduces faster procedures for removing illegal content, transparency obligations and comprehensive protection for users' fundamental rights online.
- **Digital Markets Act (DMA):** Creates new obligations for large "gatekeeper" platforms to ensure a fairer environment for business users and to make it easier for consumers to access better services and switch providers.

>ENABLING

- **Open Data Directive:** Provides the framework for reusing public sector information and facilitates access to high-value datasets to support innovation and public-interest applications.
- **Data Governance Act (DGA):** Establishes mechanisms for data sharing, public-sector data reuse and data altruism, expanding access to trustworthy data intermediaries.
- **Data Act:** Ensures fair access to and use of data generated by connected devices and services while fostering the development of a competitive and innovative data economy.

>SECURITY-ORIENTED

- **Network and Information Security Directive 2 (NIS2):** Strengthens cybersecurity and incident-response capacities across essential and important sectors.
- **Cyber Resilience Act (CRA):** Introduces cybersecurity requirements for a broad range of digital products and services, setting baseline standards for hardware and software security throughout the lifecycle.
- **Artificial Intelligence Act (AI Act):** Introduces a risk-based regime for AI systems, restricting certain practices and imposing stricter requirements on high-risk applications to promote trustworthy, human-centred AI.

Beyond shaping internal governance, this regulatory corpus has also acquired international visibility and credibility, informing regulatory debates and initiatives in several like-minded countries. As documented in cases such as Brazil,[20] elements of the EU's approach—most notably in data protection and platform regulation—have served as reference points for domestic legislative efforts seeking to reconcile digital innovation with democratic oversight and fundamental rights. This external resonance is commonly associated with the so-called "Brussels Effect," whereby access to the EU's Single Market incentivizes global firms and regulators to align with European standards. At the same time, the growing contestation of EU digital regulation, particularly by other major powers, underscores the limits of regulatory externalization and highlights that normative influence alone is insufficient to secure Europe's position in an increasingly contested digital and geopolitical environment.

Accordingly, Europe does not intend to remain a purely regulatory power; its model increasingly combines rights-centered governance with efforts to strengthen independent technological capabilities and competitiveness. The European Commission's **Digital Compass** and the **Digital Decade Program** set quantitative targets for 2030, while the **Competitiveness Compass** links rulemaking to investment in critical infrastructures, skills and industrial capacity. Proposals for a common European digital stack describe shared technological infrastructures as the cornerstone of Europe's competitiveness, ensuring that a resilient digital ecosystem reflects EU values while supporting technological leadership and long-term economic strength. Strategic initiatives, such as the **European Chips Act**, emerging investment vehicles such as **InvestAI** and proposals for a **European Sovereign Tech Fund**, illustrate how the EU seeks to onshore key technologies, mobilize funding at scale and reduce strategic dependencies, moving beyond regulation toward a more competitive and resilient position within global technology value chains.

Taken together, the EU's digital governance model combines an extensive normative framework with growing efforts to anchor regulation in technological capacity, industrial policy, and institutional enforcement. Its coherence depends not only on the breadth of its regulatory instruments, but on the Union's ability to translate rule-setting into effective control over infrastructures, markets, and implementation processes.

> It is precisely at this intersection—between regulatory ambition and material capacity—that the EU's digital strategy encounters a set of structural tensions. These tensions could undermine the internal logic of the model, because they condition its effectiveness in an international environment shaped by power asymmetries, technological concentration, and geopolitical competition.

KEY FINDINGS OF OUR ANALYSIS

03

3. KEY FINDINGS OF OUR ANALYSIS

Against this backdrop, and with the aim of helping policymakers, researchers, and industry leaders navigate an increasingly fractured digital landscape, we set out to examine how the EU—and the broader international community—can respond to the strategic pressures reshaping today's digital order. Through a series of policy papers and expert advisor meetings that span technological, economic, and geopolitical dimensions, this third work package brought together a series of analyses on themes ranging from the structural vulnerabilities of Europe's digital ecosystem to the dilemmas raised by competing governance models and the geopolitics of key enabling technologies such as data, chips, AI and payment infrastructures. The collection of papers, together with their executive briefs, have provided strategic pathways and concrete measures in this new era of digital rivalry, offering a foundation for understanding the dilemmas and opportunities facing Europe as it seeks to strengthen its competitiveness and autonomy in the global arena.

This section highlights the resulting key findings.

3.1. KEY FINDINGS OF THE THIRD WORK PACKAGE

Reclaiming Digital Sovereignty: The EU's Role in the Geopolitics of Digital Governance, *Ingrid Schneider*

In our first paper, Schneider's analysis exposes a geopolitical tension in the sphere of regulation and models of digital governance. While the United States and China have consolidated models that prioritize scale, speed, and strategic control through fundamentally different institutional paths, the EU seeks to sustain a robust rights-based governance framework in an international environment that systematically rewards regulatory flexibility and rapid technological deployment. [21]

The extraterritorial reach of the EU's regulatory measures is best articulated by Anu Bradford through the "Brussels Effect." Access to the Single Market creates strong compliance incentives for global firms to adjust their terms of service. Together with the need for interoperable systems and centralized data architectures, the Single Market encourages firms to internalize EU rules across their global operations. Through these mechanisms, EU digital regulation influences corporate behavior and governance structures internationally.

> Data protection is the major showcase for the Brussels effect. The GDPR has inspired similar legislation in many countries and is widely recognized as the international gold standard for data protection.

However, Schneider claims "Europe's regulatory influence on its own is insufficient to sustain the EU's model under conditions of intensifying geopolitical competition. It must move beyond passive regulatory influence and actively forge strategic alliances with like-minded states across the Global North and South." Furthermore, Europe's regulatory approach is at risk when it collides with the political and economic interests of great powers and even with its closest partners. In February 2025, the White House issued a formal directive authorizing responsive trade measures, potential tariffs, and scrutiny of European digital-service regulations such as the DMA and DSA for what it described as the "unfair exploitation" of American innovation.[22] This event was among the first examples of the confrontation that the Trump administration has repeatedly engaged in throughout the first year of its second mandate.

A further constraint on the EU's regulatory reach arises from the international expansion of the Chinese digital governance model, supported by strong state coordination and infrastructure control, and oriented toward strategic objectives that do not rely on alignment with EU legal standards. Much depends on whether the BRICS grow primarily as a China-centered challenger or instead as a heterogeneous set of actors whose interests do not fully converge around Beijing or Moscow. Several countries within the Global South combine criticism of Western dominance with limited incentives to support an international order shaped by Chinese or Russian priorities.

> To build resilience, Schneider's analysis points toward a strategic recalibration of the EU's regulatory power focused on coalition-building with "like-minded" partners that share a diagnosis of platform dominance and systemic digital risks.

Australia's media-bargaining rules, Japan's platform-transparency act, the UK's DMCCA,[1] and the ex-ante proposals emerging in Brazil, India, South Africa, and South Korea all reflect a shared diagnosis of platform dominance and the need to discipline the power of digital gatekeepers.

The author also warns that efforts to enhance EU competitiveness should not come at the expense of the Union's standing as a global leader in digital regulation. While rightly acknowledging an innovation gap vis-à-vis the United States and China, she cautions that weakening these regulatory frameworks could undermine trust and stability in the digital environment.

▶ Read the full Report: tinyurl.com/bpzwc3bb

1 Digital Markets, Competition and Consumers Act.

Beyond LEGO: the Need for EU-based Building Blocks of Technology, *Alexandre Ferreira Gomes, Maaike Okano-Heijmans and Jelle van den Wijngaard*

The second paper shifts the focus from regulatory frameworks to the material and infrastructural foundations of the digital economy. *Beyond LEGO* builds on the premise that digital power does not stem from individual technologies, but from the cumulative control of interdependent layers across the technology stack. Resources, chips, physical infrastructure, cloud services, data, and applications function as mutually reinforcing building blocks that shape who can innovate, who can scale, and who ultimately exercises control. The paper situates Europe's digital economy as reliant on structures it neither owns nor controls and argues that rebuilding these foundations has become essential to the Union's economic security and geopolitical agency.[23]

The structural imbalance at the heart of Europe's digital stack becomes clearest when examining the physical technologies on which it depends. More than 92% of the world's most advanced semiconductors are manufactured in Taiwanese and South Korean foundries, leaving Europe with no domestic production at the cutting edge. The vulnerability extends to earlier stages of the value chain: China refines around 90% of the rare earth elements and critical minerals needed for high-performance electronics, while much of the advanced telecom and networking hardware that underpins Europe's digital infrastructure is sourced from non-EU suppliers.[24]

Beyond physical goods, Europe relies overwhelmingly on US-based cloud providers for data storage, software services, and computational capacity. Amazon Web Services, Microsoft Azure, and Google Cloud jointly command nearly 70% of the global Infrastructure-as-a-Service market, while European providers hold barely 10%.[25] Dependency at this layer can be weaponized in at least two ways: through the withholding of services, triggering immediate operational crises, or by exploiting the threat of a cutoff to shape political or economic outcomes.

The risk intensifies when these dependencies accumulate. Taking the example of a stylized European-developed AI chatbot is useful to illustrate the remaining structural dependencies on non-European building blocks across the technology stack: it would use a model trained on hardware powered by cutting-edge chips manufactured in East Asia; run on data centers built with imported networking equipment; operate on cloud infrastructures dominated by American firms; and rely on software frameworks, programming libraries, and application interfaces that originate almost entirely outside the EU.

However, digital economic security does not require self-sufficiency across the entire technological stack, but rather the capacity to become indispensable at selected layers. The core of the EU's industrial policy should therefore focus on such strategic leverage points. For example, the European technology company ASML occupies a singular position in the global semiconductor value chain as the sole provider of extreme ultraviolet (EUV) lithography machines, a technology without which advanced chips cannot be manufactured at scale. This grants the Union control over a critical chokepoint on which all leading-edge semiconductor production depends.

Simultaneously, diversification of raw materials supply chains and hard infrastructure is best pursued hand in hand with investments in EU-based soft infrastructure. The EU would benefit from updating its public procurement laws to reflect the new geopolitical realities, prioritizing local cloud and services providers.

Existing European instruments already provide mechanisms to support industrial capacity and reduce external dependencies. The **Multiannual Financial Framework** and initiatives such as **Global Gateway** by the European Commission, channel investment toward infrastructure, industrial development, and the diversification of supply chains. Their limitation lies in their dispersion, institutional misalignment and lack of sustained economic commitment. Under these conditions, these instruments remain effective at mitigating specific vulnerabilities but insufficient to shift Europe's overall strategic position.

▶ Read the full Report: tinyurl.com/ysb5ksub

From Gatekeeper to Gameplayer: Reclaiming Europe's Strategic Relevance in the Data-Driven Age, *Dan Ciurak*

In the third policy paper, Dan Ciuriak conceptualizes the evolution of the data-driven economy as a two-phase process. The first phase unfolded during the decade of the 2010s, a period of intensive datafication characterized by widespread investment in data collection and digital infrastructure. The second phase is now underway, driven by the rise of generative and agentic AI, with equally far-reaching economic and geopolitical implications. The paper assesses why small open economies in general and the EU in particular, have lost traction in an economic revolution defined firstly by data and scale, and secondly by machine knowledge capital. Across the earlier phases of digitalization, Europe's economic model relied heavily on investment in human capital and the protection of intellectual property. These assets played a crucial role in shaping global rules during the first wave of globalization. However, in the data-driven economy, the costs of building digital infrastructure and collecting data were widely shared, while the benefits accrued to a narrow set of firms operating within large domestic markets, primarily in the U.S. and China. These firms were able to scale globally and exploit first-mover advantages in data accumulation and platform dominance.

The second, more recent phase of the data-driven economy is characterized by the rapidly growing deployment of machine knowledge capital. This form of capital substitutes for skilled labor while requiring massive investments in computation, energy resources, and advanced data centers and AI infrastructure. These features perpetuate the structural advantages of the U.S. and China, reflecting the scale dynamics of AI: the larger the data pool, the more powerful and valuable the resulting models become. Nevertheless, new actors are coming to the fore as unexpected players in the AI race, such as population-small, but energy-rich countries, including Saudi Arabia and the UAE. Meanwhile, however, the EU remains human-capital rich and energy poor while completing its transition towards decarbonization, which puts the Union at a disadvantage.

Until recently, the impact of the data-driven economy on the trading system was limited. This is no longer the case, as illustrated by mostly US-driven action. Following China's rise in data capabilities, the U.S. withdrew from e-commerce negotiations at the WTO, backed down on its support for the free flow of data and the banning of data localization requirements, imposed restrictions on connected vehicle technologies from "countries of concern," and threatened tariffs on any country that buys Huawei's Ascend AI chips.

> "This undercuts the traditional postwar trans-Atlantic alliance. The logic of realpolitik—countries have no permanent friends, only permanent interests (and even interests aren't permanent as technological conditions change)—reasserts itself."
> *—Dan Ciurak*

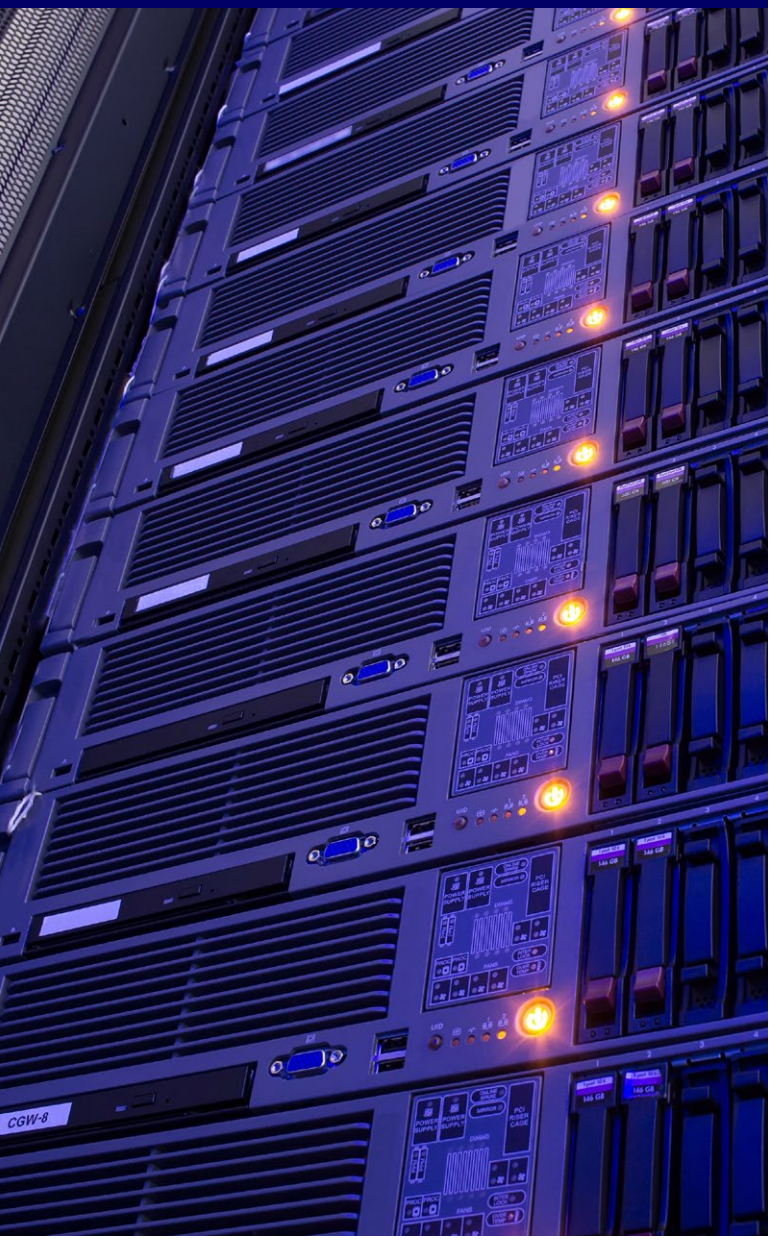
At the same time, U.S. firms have continued to benefit from business models that decouple value creation from territorial presence, limiting the ability of European authorities to tax or regulate them effectively. EU dependence on such U.S. capabilities and businesses exposes Europe to retaliation when trying to fix such fiscal and regulatory imbalances, while shared security and political commitments constrain the scope for open confrontation. This places the EU in a structurally defensive position, forced to pursue governance objectives—such as fair taxation, market contestability, and democratic resilience—within an environment where key levers of economic power lie outside its control. The renewed unilateral turn in U.S. digital and economic policy provides clear evidence of this dynamic.

Three key lessons emerge from this analysis for policymakers in Europe and beyond. **First**, the transition to the second phase of the data-driven economy must be understood as a structural reversal of the earlier levers of competitive advantage. Human capital and regulatory leadership are no longer sufficient to secure value capture; instead, control over machine knowledge capital and infrastructure has become critical.

Second, small, open economies face a systemic disadvantage when the dynamics of the data economy favour scale and capital intensity. Under these circumstances, selective concentration and institutional adaptation become unavoidable rather than optional.

Third, existing policy instruments—from large-scale investment initiatives to regulatory experimentation frameworks—should be interpreted as early responses to this shift. Their effectiveness hinges upon their integration into a coherent industrial, technological and institutional strategy capable of reconciling economic agency with security and governance constraints.

▶ Read the full Report: tinyurl.com/3hvs422z



European Monetary Sovereignty in the Digital Age, *Miguel Otero Iglesias, Paola Subbachi and Gonzalo Rodríguez*

In the last policy paper, the focus is on one of the most classical attributes of state sovereignty: the monetary and financial system. The authors Otero, Subacchi, and Rodríguez argue that the fundamental missing pillar of European monetary sovereignty is the issuance of joint debt to finance European public goods and to underpin the international role of the euro. At the same time, the increasing interconnection of payments and liquidity provision with digital technologies has opened a window for Europe to reassess its degree of strategic autonomy in the monetary and financial sphere.[26]

The debate unfolds against the global emergence of central bank digital currencies (CBDCs), understood as the only authentic form of digital money insofar as they are backed by public authority. In contrast, private digital instruments such as stablecoins and cryptocurrencies, despite their increasingly prominent role in cross-border payments and financial innovation, are not backed by any sovereign issuer, fail to perform fully the functions of medium of exchange, unit of account and store of value and thus do not constitute money in the strict sense.[27]

This evolving landscape has become another arena of geopolitical competition: China has moved rapidly with the rollout of its e-CNY, while the U.S. has taken a markedly different path by doubling down on privately issued stablecoins. Such contrast leaves open fundamental questions about the future shape of international monetary norms. In the absence of coordination and shared international standards, the global spread of CBDCs risks giving rise to fragmented and non-interoperable systems structured more by geopolitical rivalry than by global financial integration.[28]

Meanwhile, Europe remains deeply dependent on US-linked financial infrastructures, most notably SWIFT, dollar-based clearing mechanisms, and global retail payment networks such as Visa and Mastercard. Although SWIFT is formally framed as a neutral platform, its centrality in cross-border financial operations has made it a critical node of leverage.

Following the attacks of 9/11, U.S. authorities effectively integrated SWIFT into sanctions enforcement and financial intelligence architectures, blurring the boundary between technical systems and instruments of statecraft.[29]

The coercive potential of this architecture became particularly visible after the reactivation of U.S. sanctions against Iran. Exclusion from SWIFT, c ombined with the threat of secondary sanctions and restricted access to dollar clearing, led major European firms—including Total, Siemens, and Peugeot—to rapidly cease operations in the country, despite the EU's formal opposition to these measures.

Against this backdrop, the digital euro emerges as a necessary but insufficient response. Together with the global dominance of Visa and Mastercard in retail payments, Europe's dependence on foreign systems highlights the need to modernize its monetary framework and to reduce external vulnerabilities. The digital euro is therefore presented as an important step toward equipping the euro with a more autonomous payments infrastructure, based on a hybrid model that ensures pan-European reach while fostering European private solutions and infrastructures. [30] A step forward in building a real European payment system is the European private agreement to enable cross border interoperability of instant payment solutions.[31]

A solution that offers a fast and practical way to strengthen Europe's payment resilience and strategic autonomy, by leveraging proven infrastructure, strong consumer adoption, and private sector innovation, supporting work on the digital euro. This initiative demonstrates the capacity of Europe's private sector to work together successfully to deliver concrete, scalable solutions at speed and at scale, in support of Europe's broader monetary and strategic objectives, and to the benefit of European citizens.

> Yet, without permanent EU bonds and a credible common fiscal capacity, the international attractiveness of the euro—and by extension the strategic impact of the digital euro—will remain curtailed.

The issuance of joint debt, the completion of the banking and capital markets unions, and the development of resilient European financial infrastructures are interdependent. Only when combined can they allow Europe to move beyond regulatory authority and limited payment autonomy toward a more robust form of monetary sovereignty, capable of withstanding external coercion and supporting precisely the strategic autonomy needed in an increasingly weaponised financial system and world economy.

▶ Read the full Report: tinyurl.com/4n7h92v4

3.2. EUROPE'S STRATEGIC DILEMMAS

Considering the different analyses developed during this third work package, we present here a series of strategic dilemmas that the EU will have to tackle in the years to come:

Regulatory power **vs** Material power

EU regulatory instruments such as the GDPR, DMA, and DSA have shaped legislative debates and informed regulatory reforms in countries including Brazil, Mexico, South Africa, and India, illustrating how the Union's rule-setting capacity operates as a form of unilateral soft power. This influence, however, unfolds in an environment where regulatory authority is increasingly conditioned by material capabilities.

Digital power is concentrated in platforms, semiconductor capacity, cloud infrastructure, and large-scale data systems—domains in which the U.S. and China retain structural advantages. In this context, alignment based on normative appeal alone has become less decisive. Governments that draw inspiration from EU rules often balance this orientation against pressures from Washington, incentives from Beijing, and the risks associated with technological dependence.

The resulting dilemma is whether Europe's regulatory and value-based influence can remain globally effective, as well as desirable as a core objective of the European digital governance system, in the absence of a stronger technological and economic foundation. It also questions to what extent regulatory soft power can offset structural gaps in critical digital capabilities under conditions of sustained geopolitical competition.

Economic openness and interdependence **vs** security and control

The EU's economic and technological model has been shaped by a high degree of openness, resulting in a technology stack that is largely outsourced across multiple layers, including cloud services, semiconductors, and critical digital infrastructures. This configuration has supported innovation and market integration, but it has also generated structural dependencies on non-EU providers and production locations, exposing the Union to vulnerabilities related to continuity of services and economic security.

Beyond LEGO documents how such dependencies can be weaponized through the withholding of essential technologies or the threat of restricting access, turning interdependence into a channel of leverage rather than mutual resilience. Reliance on US-based cloud providers, concentration of advanced semiconductor manufacturing in a limited number of non-European locations, and exposure to external constraints along global supply chains, where China has a dominant presence from critical raw materials to green tech, illustrate how control over key building blocks increasingly conditions autonomy. In response, the EU and its member states have begun to reassess openness as a governing principle, promoting supply-chain diversification, selectively onshoring critical capacities, and encouraging the relocation of sensitive and vital societal functions toward EU-based providers.

The resulting dilemma is how Europe can preserve the economic benefits of openness while reducing one-way dependencies that can compromise its security and essential service provision across the technology stack, in a context where economic security, digital sovereignty, and geopolitical leverage are becoming increasingly intertwined. Ultimately, economic security comes at a cost.

Alliances **vs** strategic autonomy

The EU's position in the digital economy depends heavily on cooperation with external partners. Access to advanced semiconductors, cloud services, and other critical inputs is closely linked to security, trade, and technology arrangements with the U.S. and key partners in Asia; cooperation with like-minded democracies in regions such as Latin America, Africa, and the Indo-Pacific supports the diffusion of rights-based approaches to digital governance.

These alliances serve multiple functions: they help compensate for Europe's limited material power in key digital domains, amplify the reach of its regulatory preferences, and reduce one-sided dependencies on either Washington or Beijing. At the same time, alignment with major powers introduces constraints. Pressures to follow U.S. export controls, (over)reactions to EU technology regulation both from the U.S. and China, and competing infrastructure and investment offers can narrow Europe's room for manoeuvre and complicate efforts to pursue independent policy choices.

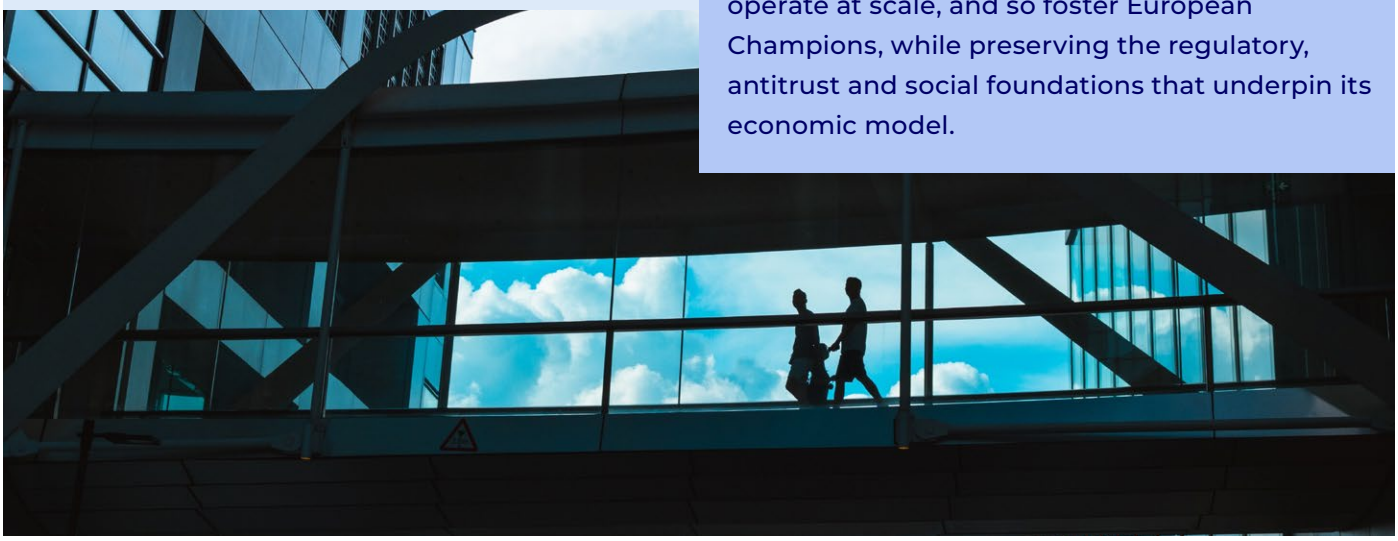
The resulting dilemma is how Europe can deepen the alliances it relies on for access, influence, and diversification while preserving the capacity to define autonomous positions when its economic or political interests diverge from those of its main partners.

Scale and competitiveness **vs** fragmentation and social welfare

Europe's ability to generate scale in the digital economy is constrained by persistent fragmentation within the Single Market. This diagnosis is explicitly highlighted in the Draghi Report on European competitiveness. Divergent regulatory requirements, administrative barriers, and limited coordination across Member States restrict firms' ability to expand across borders and achieve scale comparable to global competitors. These constraints, combined with underinvestment and sectoral silos, shape a business environment in which the emergence of large, globally competitive European firms (the so called European Champions) remains difficult.

At the same time, the regulatory features often associated with fragmentation—rights-based protections, high standards, and protection of certain regions, sectors, professions and public services—also constitute central elements of the European economic and social model. Experiences in countries that have drawn inspiration from EU digital regulation suggest that weakening such safeguards in the name of competitiveness can erode institutional trust and diminish the model's external credibility as a reference point for digital governance.

The resulting dilemma is how Europe can reduce internal fragmentation and enable firms to operate at scale, and so foster European Champions, while preserving the regulatory, antitrust and social foundations that underpin its economic model.



Capturing data and AI rents **vs** safeguarding democracy and rights

In the data-driven economy, value capture rests on the ability to transform large-scale datasets and AI systems into a form of productive capital. The rents associated with this "machine knowledge" shape competitive positioning and fiscal capacity, as firms and large economies consolidate control over digital infrastructures and the intangible assets built upon them.

For the small open economies that constitute the EU, participation in this regime is a structural condition rather than a policy choice. Limited access to data aggregation, compute, and large-scale AI deployment constrains the capacity to capture data and AI rents and reinforces asymmetric positioning within the global digital economy.

At the same time, the architectures that enable rent extraction also reconfigure the information environment of open societies. Continuous data capture, behavioural targeting, and AI-mediated curation increase the legibility of social behaviour while expanding exposure to manipulation, polarization, and information operations. Europe's rights-based governance framework operates as a constraint on these dynamics, but it also conditions the scale and reuse of data required for advanced AI applications.

These tensions are not only economic or technological, but they also directly shape the conditions of democratic legitimacy, social cohesion, and institutional trust in Europe. In this sense, the struggle over data governance and AI infrastructures is inseparable from the broader question of how a democratic social contract can be sustained in the digital age.

The resulting dilemma is how European democracies can capture a share of data and AI rents while maintaining institutional safeguards that prevent the erosion of social cohesion and democratic self-government.

Public-sector initiative **vs** private-sector initiative

Across multiple strategic domains, Europe's governance model relies on a complex interaction between public authority and private initiative. Market-driven solutions often develop effectively at the national or sectoral level but struggle to scale across borders, while public infrastructures and regulatory frameworks do not always align with private incentives to invest, standardize, and deploy interoperable systems. This configuration contributes to persistent fragmentation and limits the emergence of shared European capacities.

Many of the building blocks on which European sovereignty increasingly depends—including digital infrastructures, data ecosystems, cloud and compute capacity, identity frameworks, and other foundational services—require a dual dynamic. Public institutions are needed to define common architectures, standards, governance frameworks and initial funding and act as early adopters, while private actors provide capital, innovation, and operational deployment. Coordination across these actors, however, is conditioned by uneven fiscal capacities, divergent market structures, and differing political priorities across Member States, which complicates collective action and slows convergence.

Under these conditions, Europe's challenge is not a choice between public and private initiative, but the ability to embed both within genuinely European architectures rather than allowing them to remain confined to national, sectoral, or firm-level silos.

The resulting dilemma concerns how public authority and private innovation can be mobilized simultaneously to build shared capacities, reduce structural dependencies, and strengthen Europe's ability to exercise control over critical infrastructures across domains.

DIGITAL GEOPOLITICS AND THE NEW SOCIAL CONTRACT

04

4. DIGITAL GEOPOLITICS AND THE NEW SOCIAL CONTRACT

The strategic dilemmas identified in the previous section are not only geopolitical or economic in nature. Taken together, they point to a deeper challenge: the gradual misalignment between digital transformation, political authority, and the social foundations of democratic legitimacy. In this sense, the geopolitics of the digital domain is inseparable from the question of the **social contract in the digital age**.

Historically, social contracts in advanced economies have rested on a relatively stable bargain. Economic openness, technological change, and market integration were accepted insofar as public institutions retained the capacity to provide security, redistribute gains, correct market failures, and protect citizens from excessive risk. Digital transformation is straining this bargain. The scale, speed, and concentration dynamics of the digital economy have weakened the link between value creation and territorial governance, while simultaneously increasing societies' dependence on infrastructures and actors that escape democratic control.

This tension is now amplified by geopolitics. As digital technologies become instruments of power projection, coercion, and strategic competition, states' capacity to uphold the implicit promises embedded in their social contracts increasingly depends on their position within power structures, global digital value chains and governance regimes. The strategic dilemmas facing Europe therefore translate directly into social and political dilemmas about trust, fairness, and democratic agency.

FROM STRATEGIC DILEMMAS TO SOCIAL LEGITIMACY

Several of the dilemmas identified earlier acquire their full significance when viewed through the lens of the social contract.

The tension between **regulatory power and material power** is not merely an institutional concern. Rights-based regulation is a central pillar of Europe's social contract in the digital age, expressing collective expectations regarding privacy, fairness, accountability, and human dignity. However, when regulatory ambition is not matched by enforcement capacity and material control over infrastructures, it risks being perceived as symbolic rather than effective.

> A social contract cannot be sustained if citizens observe that rules exist but cannot be meaningfully imposed on the actors that shape their digital environment.

Similarly, the dilemma between **economic openness and security** has direct social implications. Europe's openness has supported growth and integration, but it has also produced structural dependencies that expose societies to external shocks and coercive leverage. When essential digital services, cloud infrastructures, or payment systems are vulnerable to disruption beyond European control, the ability of public authorities to guarantee continuity, stability, and protection is weakened. Over time, this undermines confidence in the state's capacity to act as a guarantor of collective security in the digital domain.

The dilemma between **alliances and strategic autonomy** also carries social consequences. While alliances remain indispensable, excessive dependence on external partners can narrow Europe's policy space in areas that directly affect citizens, such as data governance, competition, taxation, and industrial policy. When democratic choices appear constrained by external technological or geopolitical pressures, the legitimacy of political decision-making erodes, feeding perceptions of powerlessness and disengagement.

Finally, the tension between **scale and competitiveness on the one hand, and national fragmentation and social protection on the other**, speaks to the core of Europe's economic and social model. Digital competitiveness increasingly rewards scale, concentration, and capital intensity, while Europe's regulatory and welfare frameworks are designed to protect pluralism, economic competition, regional balances, and social cohesion. If digital transformation is experienced primarily as a force that concentrates rents at the top and abroad while imposing adjustment costs domestically and at the bottom of the income distribution, the social acceptance of openness and innovation is likely to weaken.

DIGITAL SOVEREIGNTY AS A SOCIAL CONTRACT ISSUE

Against this backdrop, digital sovereignty emerges not only as a strategic objective, but as a precondition for renewing the social contract in the digital age. Digital sovereignty, as developed throughout this report, refers to the capacity of a political community to make autonomous decisions about its digital environment, guided by democratic values and strategic priorities. This capacity underpins the credibility of the social contract. Without sufficient digital sovereignty, public authorities struggle to fulfil core social functions and promises. Fair taxation becomes more difficult when value creation is detached from territorial presence. Redistribution weakens when digital rents are concentrated at the top and captured externally. Labor market transitions become harder to manage when innovation ecosystems are located elsewhere and technological innovation is not well disseminated. Democratic accountability erodes when key infrastructures are governed by foreign legal regimes or opaque corporate decision-making.

> Conversely, strengthening digital sovereignty enhances the ability of democratic institutions to shape technological change in line with social objectives.

Regulatory frameworks gain legitimacy when they are enforceable. Industrial and innovation policies become socially meaningful when they generate domestic value creation, employment, and skills. Investment in critical infrastructures supports resilience not only at the strategic level, but also in citizens' everyday economic lives. In this sense, the four pillars of digital sovereignty identified in this report correspond to foundational elements of a renewed social contract. Regulatory capacity and norm-setting power articulate collective values and expectations. Control over key layers of the technology stack anchors economic activity within the European social and territorial framework. The ability to capture value from data and AI underpins distributive fairness. The resilience of monetary and financial infrastructures sustains trust in the economic system as a whole and protects against foreign coercion.

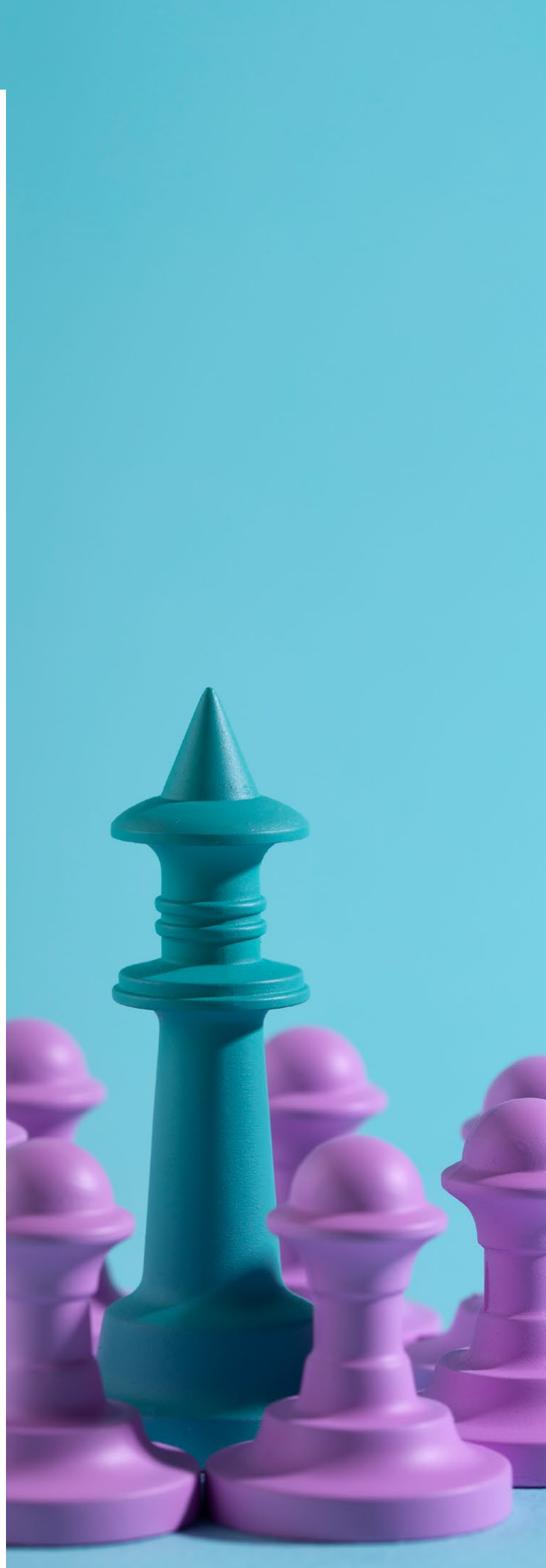
THE POLITICAL ECONOMY OF TRUST IN THE DIGITAL AGE

The erosion of the social contract is not an abstract risk. Across Europe and beyond, dissatisfaction with digital platforms, concerns about surveillance, manipulation and addictions (from a young age), and anxieties about economic insecurity are increasingly reflected in political polarization and declining trust in institutions. These dynamics are often framed as cultural or informational phenomena, but they are deeply rooted in political economy.

When societies perceive that technological transformation benefits a narrow set of actors while weakening public capacity and individual and social protection, support for democratic governance diminishes. In this context, digital governance is not only about managing risk or promoting innovation, but about sustaining the material and institutional conditions under which democratic consent remains viable.

The emphasis here on material capabilities, infrastructural control, and value capture is therefore not technocratic. It reflects an understanding that social legitimacy in the digital age depends on visible state capacity. Citizens are more likely to accept digital transformation when they perceive that public institutions retain agency, that rules are enforceable, and that economic gains are not highly concentrated and systematically externalized.

The strategic dilemmas identified earlier are not choices between abstract policy options, but political economy tensions that shape the lived experience of digitalization for European societies. The recommendations that follow should therefore be read not only as instruments to enhance Europe's geopolitical position, but as components of a broader effort to restore alignment between digital transformation, democratic governance, and social cohesion. The challenge for Europe is not simply to compete in the digital domain, but to ensure that digital change remains compatible with the social and political foundations on which the European project rests.



RECOMMENDATIONS

05

5. RECOMMENDATIONS

PILLAR 1 — REGULATORY CAPACITY AND NORM-SETTING POWER

INTERNAL ACTION

01 Personify EU's Digital Leadership

Developing a comprehensive and unified digital policy requires strong guidance, one that is both visible and personified through:

- Appointing a special representative, envoy or ambassador-at-large for digital affairs to provide political leadership, synergize the EU's efforts, articulate core concerns and foster dialogue with partner countries. The appointee should serve as a bridge-builder between the different Commission portfolios—such as trade, internal market, tech sovereignty and economic affairs. It should also leverage the network of EU delegations to identify key issues influencing partners' digital policies. He or she should also represent the EU in all international fora on digital matters, ensuring a unified and strategic voice. Their work should fall under the joint supervision of the Executive Vice-president of the European Commission for Technological Sovereignty, Security and Democracy, Henna Virkkunen, and High Representative for Foreign Affairs and Security Policy, Kaja Kallas, ensuring alignment with the EU's digital policy objectives and technological competitiveness.
- Expanding the network of digital attachés in key EU delegations (US, China, Brazil, India, Mexico, South Africa, Indonesia and others) to ensure effective communication and alignment with allies, as well as provide support for third countries looking to align their digital policies with European standards.
- Enhancing the role of European Parliament committees in promoting EU digital norms by engaging in regulatory discussions with global partners through the committees of foreign affairs, civil liberties and industry, and inter-parliamentary forums.[32]

02 Promote fundamental rights, values and European regulatory standards through effective enforcement

To achieve global resonance, the EU must implement at home its digital regulations in a comprehensive, coherent and consistent manner by:

- Ensuring horizontal coordination between the different Directorates-General (DGs)—including DG COMP, DG CONNECT, DG JUST and DG TRADE—as well as vertical collaboration with regulatory agencies—such as the European Data Protection Supervisor (EDPS)—and national authorities in charge of implementing digital regulations to achieve cross-compliance[33].
- Providing adequate funding and competent workforce for new EU agencies like the AI Office to implement the AI Act and other legislative frameworks effectively.
- Providing technical support and guidance to businesses, particularly SMEs, to help them comply with legislative requirements.

EXTERNAL ACTION

03 Enhance multilateral cooperation and various digital governance coalitions in the Global North and South

The EU is not alone in its efforts to regulate digital markets and the unchecked power of global tech giants. Strengthening partnerships with like-minded democracies and emerging digital economies globally can significantly support the EU's "third way" digital governance strategy by:

- Intensifying current partnerships to foster a safe and inclusive digital space with Japan, South Korea, Singapore and Canada, fostering mutual exchange of best practices and regulatory experiences, and expanding these partnerships to more like-minded countries. [34]
- Forming various coalitions with regional, state and non-state actors based on shared support for specific policy frameworks, such as the human-centric digital transition or digital public infrastructures. The members of each coalition should be engaged in proper consultations and peer-review mechanisms, embracing others' ideas to develop more inclusive and globally aware digital policies[35].
- Adopting a proactive role in multilateral fora and trade agreements, ensuring that digital chapters reflect its values and priorities. The follow-up- and review-processes of the UN Global Digital Compact will be an opportunity for the EU to continue engaged and to safeguard human rights standards, multistakeholder collaboration and public digital infrastructures. [36]
- Replicating the successful framework of the EU-Latin America and Caribbean Digital Alliance[37] by initiating similar partnerships with the African Union and ASEAN. Focus on capacity-building to help develop digital skills and infrastructure in local economies, work together to develop regulations that promote fair competition and consumer protection, and promote joint initiatives for research and development in digital technologies.

04 Reinforce the Global Gateway program

The Global Gateway program has come under substantial criticism for being predominantly aspirational and for its heavy reliance on existing programs.[38] This reliance raises concerns about its capacity to offer a genuinely competitive counterbalance to China's Digital Silk Road.

The EU should reinforce this program by:

- Incorporating a robust regulatory component linked to the EU's digital policy and digital diplomacy objectives in close collaboration with partner countries to support rules-based institutions.[39]
- Prioritizing investments in strategic corridors, which have proven effective in enhancing regional connectivity and economic integration. Increasing investments in AI and semiconductors, and complementing these with digital connectivity projects, can further amplify the effectiveness of these corridors.[40]
- Establishing comprehensive regulatory and technological cooperation frameworks that extend beyond mere physical infrastructure. Allocating funds for scientific cooperation and technology development is crucial. Additionally, strengthening connections with civil society organizations will foster sustainable and inclusive partnerships, reinforcing the EU's strategic objectives globally.

PILLAR 2 — CONTROL OF THE TECHNOLOGY LAYERS (DIGITAL BUILDING BLOCKS)

To move beyond regulatory protection and address structural dependencies, the EU should strengthen European indispensability in key technological nodes and strategically focus investment on areas of competitive advantage.

INTERNAL ACTION

01 Support European cloud and AI champions through strategic resource access

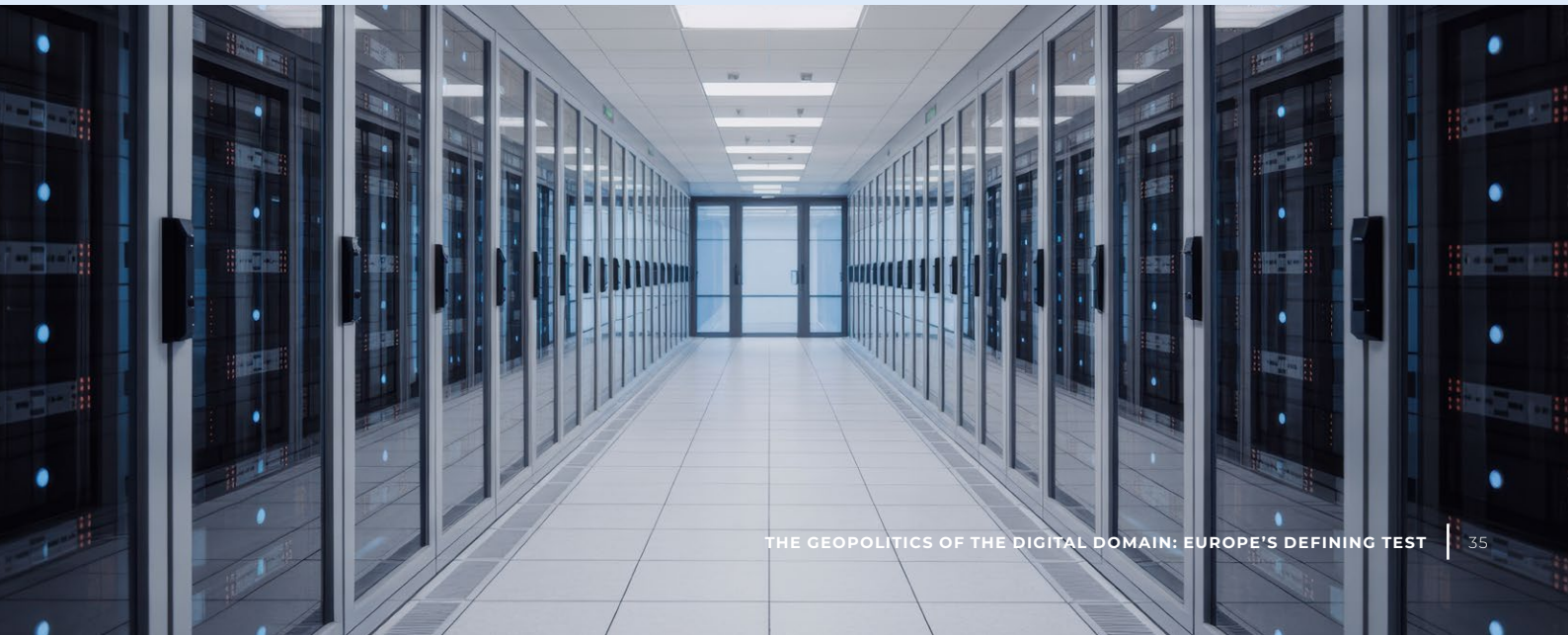
To strengthen Europe's soft digital infrastructure, the EU should:

- Prioritize support for European cloud and AI providers such as STACKIT, OVHcloud, and IONOS, enabling them to scale and compete globally in a market currently dominated by US platforms.
- Ensure that these providers have access to energy, water, and land for building data centers and "AI factories," essential for developing large-scale, sovereign infrastructure.
- Internalize the externalized environmental and economic costs of foreign-owned infrastructure, ensuring European resources do not disproportionately support non-European profits.
- Use the upcoming AI and Cloud Development Act to define clear rules for ownership, transparency, and concession models, promoting digital sovereignty and long-term infrastructure resilience.

02 Leverage public procurement to scale European cloud providers

To strengthen the market position of European cloud services, the EU should:

- Revise EU public procurement frameworks to explicitly favor European providers in sensitive sectors such as healthcare, education, and public administration, ensuring data protection and sovereignty.
- Direct institutional demand toward viable European solutions to help overcome market fragmentation and scale disadvantages faced by domestic providers.
- Use procurement not merely as a budgetary tool, but as a strategic policy instrument to accelerate the growth of a competitive and autonomous European cloud ecosystem.



03 Augmenting European indispensability through strategic investment

European indispensability in global value chains is one of the most effective strategies for securing digital sovereignty. The case of ASML, which holds a unique position in advanced chipmaking equipment, illustrates the importance of controlling critical technological nodes that are difficult or impossible to replace. To replicate this model in other areas, the EU should:

- Direct public investment toward chokepoint technologies where it already has a competitive edge or high growth potential.
- Coordinate funding instruments under the Multiannual Financial Framework (MFF) and focus on creating non-substitutable capacities. This includes prioritizing areas of high geopolitical leverage, supporting research and scale-up, and reducing dependency on external partners in foundational layers of the digital stack.

EXTERNAL ACTION

04 Engaging the U.S. on data localization and shared standards

U.S. legislation such as the CLOUD Act and FISA raise concerns about privacy and extraterritorial access to data. While the risk of misuse under the American laws may be low in normal conditions, data can easily be weaponized, posing serious risks in times of geopolitical tension. In light of this, the EU should:

- Encourage the repatriation of sensitive data to European providers.

05 Leverage partnerships with India, Japan, and Association of Southeast Asian Nations (ASEAN)

The EU should expand partnerships with India, Japan, and ASEAN to advance a democratic and de-risked digital order by:

- Promoting trilateral cooperation and expanding bilateral platforms such as the EU–India Trade and Technology Council and the EU–Japan Strategic Partnership to foster regulatory alignment and technological cooperation.
- Collaborating with ASEAN to establish baseline standards for interoperability and connectivity, addressing the region's limited capacity to deploy fiber optics and 5G simultaneously.
- Supporting joint digital infrastructure and skills initiatives through the Global Gateway, building on the 2023 Joint Ministerial Statement on Connectivity and newly announced projects tailored to local needs.

06 Diversify CRM sources and co-develop extraction capacity in Africa and Latin America

To reduce strategic dependencies on China in critical raw materials (CRMs), the EU should:

- Implement its MoUs with Chile, Zambia, and the Democratic Republic of Congo, focusing on lithium, cobalt, and rare earths that are vital for Europe's digital and green transitions.
- Use the Global Gateway to mobilize blended finance and ensure that CRM projects contribute to local industrial processing, not just resource extraction.
- Offer a credible alternative to China's Belt and Road Initiative by embedding transparency, environmental safeguards, and shared economic benefits into its global resource partnerships.

07 Strengthen supply chain resilience through targeted, business-driven partnerships

To ensure successful external digital and CRM strategies, the EU should:

- Engage businesses from the outset of project design to ensure initiatives are aligned with market needs, commercially viable, and strategically relevant.
- Leverage the Global Gateway's digital pillar as an operational entry point, offering tailored technical assistance and investment to support local capacity-building.
- Involve EU Member States in identifying the strengths of partner countries' tech sectors, and co-develop small-scale, sector-specific projects that are adapted to local contexts—avoiding generic megaprojects.

PILLAR 3 — THE CAPACITY TO CAPTURE BENEFITS FROM THE DIGITAL ECONOMY

These recommendations outline steps the EU, in collaboration with small open economies, can take to reduce vulnerabilities and improve economic outcomes in the data- and generative AI–driven economy:

INTERNAL ACTION

01 Support domestic firms in the data and generative AI economy with the capacity to scale

Public policy should shift from fragmented support for innovation inputs to targeted interventions that enable the emergence of European industrial champions/superstars in the digital domain by:

- Refocusing industrial and digital strategies on scaling firms by shifting performance metrics from inputs (e.g., support for research or infrastructure funding) to scaling outcomes, such as numbers of firms meeting high-growth criteria. The tracking of unicorns in the European Commission's *State of the Digital Decade* report is a start.
- Supporting the creation of AI consortia, joint ventures, and strategic mergers among Europe's fragmented industrial AI start-up ecosystem through regulatory reforms (e.g., competition policy flexibility for strategic sectors, a refocus of the EU FDI regulation on the economic impact of M&A activity on the European population of AI firms) to prevent the absorption of EU-generated rents by foreign platforms.
- De-risking private investments by signalling clear national and EU-level priorities through large, visible public sector investment commitments (e.g., InvestAI's €200bn fund is a step in this direction) in strategic sectors to reduce scaling bottlenecks.
- Create strong European initiatives to find, attract, train and develop European and international human capital, at the time when many top researchers in the U.S. are looking for new horizons.

02 Develop palliative responses to backwardness in the data and predictive AI economy

As Europe positions itself in the emerging data and generative AI economy, it must also address legacy vulnerabilities created during the previous phase, which left it dependent on foreign digital infrastructure and software ecosystems, by:

- Prioritizing the reversal of the decline in Europe's share of its domestic cloud market to increase Europe's capture of data and AI rents, attenuate its growing strategic vulnerability, and pre-emptively reduce frictions from attempts to claw back data and AI rents through taxation of foreign platforms. This can be jump-started through increased public procurement of EU-based software and cloud services, justified on essential security grounds to create demand-side pull for domestic alternatives.
- Advancing initiatives like DNS4EU to strengthen capabilities within other layers of the digital stack, aligning with the advocacy of the EuroStack initiative. Focus both on hardware but also software, an underinvested field in Europe.
- Framing these efforts around cybersecurity, rent capture, and strategic autonomy—not protectionism—to avoid the geopolitical friction created by digital services taxes and competition policy penalties.

03 Reconceptualize the value of data as a strategic asset

To capture the full value of data and enable a competitive, scalable innovation ecosystem, the EU must rethink both its economic and governance approach to data by:

- Shifting data valuation frameworks used by national statistical authorities and tax systems from cost-based methods (i.e., cost of datafication) to value-based approaches that reflect the economic rents data enables when embedded in AI models, platforms, or analytics, to prevent misguided policy.
- Building a secure, industrial-scale European and allied data-sharing space to reach the scale that is essential to effectiveness and the generation of economic rents. Leverage the GDPR's adequacy framework to extend the data-sharing zone to trusted partners—such as Canada—with aligned governance standards.
- Establishing clearly defined regulatory sandboxes for high-impact, high-reward AI applications, acknowledging that risk and reward are inseparable, and enabling experimentation with use cases like autonomous vehicles that support value capture through deployment.

EXTERNAL ACTION

04 Safeguard and reinforce the technical institutional acquis for a full post-conflict reboot

In an era marked by intensifying geopolitical competition and institutional erosion, the EU must act decisively to preserve the integrity of global technical institutions and prepare the ground for a functional reboot of the international order by:

- Mobilizing coalitions of small open economies to defend the neutrality and continuity of global technical institutions—such as IEEE, ITU, and ICANN.
- Continuing to respond to geopolitical trade disruptions and unilateralism by leading powers by reforming multilateral institutions like the WTO or by creating new ones among like-minded middle powers.
- Collaborating with groups of small open economies such as the Ottawa Group to advance 21st-century trade reforms that reflect the realities of AI, data, and platform economies—drawing on work from the OECD (Going Digital), the WTO (Trading with Intelligence), and the broader epistemic community.

05 Work towards identifying a stable "landing zone" for the post–Pax Americana digital economy

Recognizing that political institutions are creatures of their age, the EU should lead efforts to lay the conceptual and diplomatic groundwork for a rebalanced international order by:

- Launching a Track 2 process to articulate interim cooperation frameworks—such as an Interim Solution on Tariffs and Trade (ISST) and an Interim Solution on Money and Exchange (ISMX)—that offer the basis for short-term governance while establishing the intellectual foundations for a new political architecture that the United States and China could conceivably buy into, while also serving the interests of small open economies.
- Convening a multilateral dialogue to define a shared "landing zone" for the digital economy. This would involve an inclusive, forward-looking conference, modeled on the 1933 London Conference under the auspices of the League of Nations, focused on addressing today's equivalent systemic breakdown: the lack of consensus on trade and bilateral trade imbalances, exchange rates and payments systems, and the governance of the digital economy—including data and AI rent-sharing and trade in connected devices.

PILLAR 4 — ADAPTABILITY OF CRITICAL DIGITAL INFRASTRUCTURES

These recommendations set out how the EU can strengthen its monetary sovereignty by reinforcing the foundations of the euro—through safe assets, joint debt issuance, and integrated financial markets—while adapting its monetary and payment infrastructures to an increasingly digital environment.

INTERNAL ACTION

01 Build scale and safe assets

Europe needs depth and trust in its financial system. A pan-European safe asset, stronger capital mobilization, and a digital euro designed to complement—not replace—market reforms are essential foundations.

- Issue, in sufficient volume, a pan-European sovereign risk-free asset to complete the capital markets union and foster cross-border investment.
- Leverage the window of distrust in the dollar to repatriate European capital currently invested in the U.S. and accelerate EU bond issuance.
- Create a hybrid strategic investment fund blending EU-issued bonds with private capital to mobilize resources for innovation—inspired by Draghi's call for joint funding of European public goods and private co-investment.

02 Deepen and integrate markets

Fragmentation prevents the euro from reaching global weight. Completing the banking union, harmonizing rules, and reinforcing and developing own payments systems can unlock a more unified financial space.

- Complete the banking union and capital markets union, newly called savings and investments union, to foster greater cross-border investment and the creation of pan-European banks.
- Harmonize financial regulation, tax policy, bankruptcy law, and infrastructure investment to create the foundations of a global financial center.
- Establish a "28th business regime" to overcome the national roadblocks that exist toward harmonization through the enhanced cooperation instrument, starting with initiatives like Spain's Competitiveness Lab and a harmonized credit rating system for SMEs.

03 Diversify liquidity and payment infrastructures

Resilience requires alternatives. Expanding euro swap lines, curbing extraterritorial risks, and developing both external and home-grown payment systems will reduce dependence.

- Scale up euro-denominated swap agreements with central banks to diversify the global financial safety net away from exclusive dollar and U.S. reliance.
- Strengthen and expand the TARGET2 payments system, uniting mobile payment systems across Member States.
- Monitor emerging payment systems outside the EU and U.S. (CIPS, ASEAN LCS) to assess risks to European sovereignty.
- Support and promote European-led payment initiatives that can scale across Member States and ensure interoperability, reducing reliance on non-European networks (e.g., EU Wero and EuroPA).
- Promoting, if possible, private initiatives on payments to enable cross border interoperability of instant payment solutions. A solution that offers a fast and practical way to strengthen Europe's payment resilience and strategic autonomy, by leveraging proven infrastructure, strong consumer adoption, and private sector innovation, while supporting work on the digital euro.

04 Secure legitimacy, political momentum, and strategic autonomy

- Ensure the social legitimacy of the digital euro through transparent and pedagogical communication that clearly conveys its benefits and safeguards to both citizens and the European Parliament.
- Use the political momentum of the digital euro debate to advance fiscal and capital markets unions, consolidating European monetary sovereignty and strengthening the euro's global role.
- Promote international legal frameworks to limit unilateral sanctions, with transparency and multilateral oversight.

EXTERNAL ACTION

05 Strengthen the euro's international attractiveness

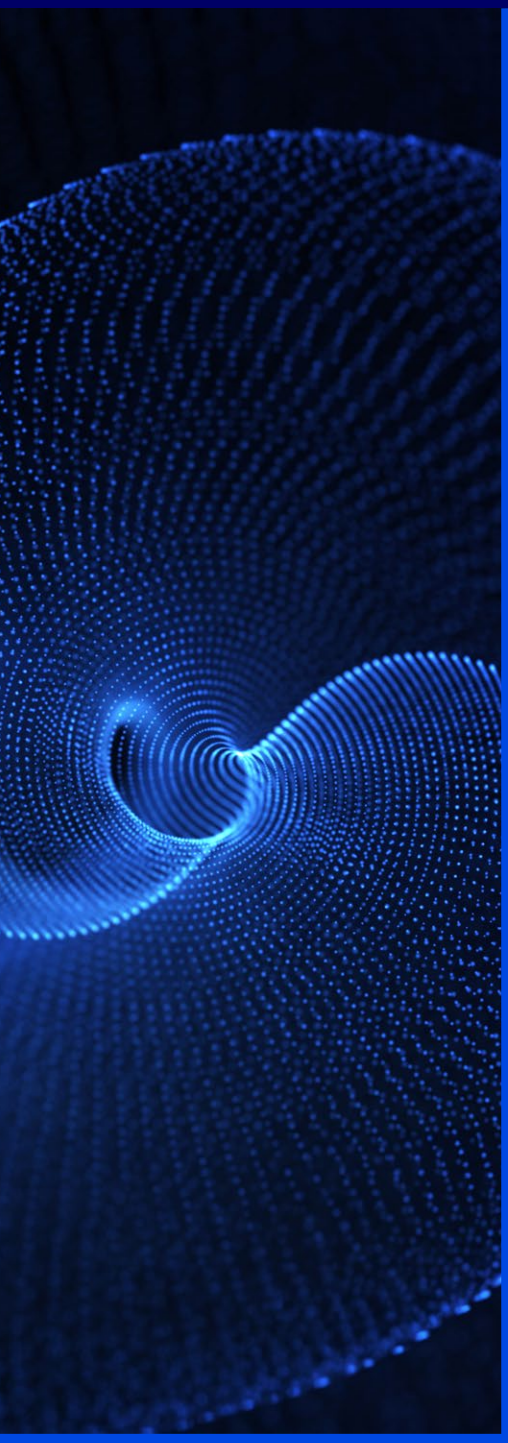
To rival the dollar, Europe must provide a credible alternative for global investors. Advancing fiscal and market integration, coupled with scaled-up EU bonds directed at common public goods, would anchor the euro as a trusted global currency.

- Expand euro-denominated swap lines and develop alternative liquidity frameworks to reduce dollar dependence and vulnerability to US geopolitical leverage.
- Focus EU joint debt issuance on strategic European public goods and projects of common interest, given resistance by some Member States to a full fiscal union, financing them through EU-level instruments rather than broad fiscal integration.
- Issue EU bonds as much as current capacity allows, extending the Next Generation EU model to finance European public goods such as energy networks or deep tech, to offer global investors a credible alternative to U.S. Treasuries.

06 Accelerate the development of the digital euro

The digital euro is central to Europe's monetary future. Its design and deployment must move forward, supported by pilot testing, global coordination, and a strong legal base to ensure resilience and competitiveness.

- Accelerate technical preparation and political consultation on the digital euro and begin pilot testing in both retail and wholesale forms.
- Build the digital euro on a strong European legal framework, democratically legitimized and flexible in its implementation, to prevent political blockages or regulatory rigidities that could hinder innovation.
- Increase international consultation and coordination with other jurisdictions advancing in CBDCs, using the opportunity to take first-mover advantage in setting standards, security protocols, norms, and interoperability.



CONCLUSIONS

06

6. CONCLUSIONS

The digital domain has become a core environment of geopolitical competition. Digital technologies are no longer peripheral instruments of modernization, but enabling infrastructures that shape economic power, military advantage, societal resilience, and strategic influence. Because these technologies underpin virtually all other sectors, leadership in areas such as artificial intelligence, semiconductors, cloud computing, data governance, and digital payments has become a central ambition of states and a decisive axis of global rivalry. The Pax Silica[41] proposed by the U.S. is the latest example of this trend.

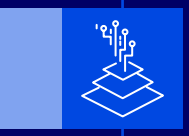
For the European Union, this shift marks a moment of strategic realization. Europe's model has been built primarily on regulatory power, social cohesion and the projection of democratic norms, rather than on ownership and control of the critical technological capabilities that structure the digital economy. The EU has exercised significant influence through its rights-based governance framework, shaping global debates on privacy, platform accountability, competition, and trustworthy AI. Yet regulatory authority alone is proving insufficient in an international environment where sovereignty is increasingly conditioned by military conflict, material capabilities, technological scale, and infrastructural control.

The great challenge for the EU in the coming years is balancing external and internal security with social cohesion.[42] The geopolitical context of great power rivalry and the dynamics of the digital economy confront Europe with deep strategic dilemmas which will shape the new social contract necessary to have a more stable socioeconomic and political future. Digital sovereignty has become indispensable not only for insulating European societies from external coercion, but also for preserving agency over the kind of digital ecosystem, economic model, and social contract that Europeans will inhabit. The EU is attempting to navigate these dilemmas in a critical moment of change, as technological competition intensifies and alliances become more volatile.

In this context, Europe must act across four interconnected domains, both within the Union and beyond its borders, in close cooperation with international partners.

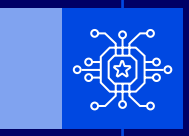
01/

First, Europe must reclaim its regulatory capacity and norm-setting power, without backsliding through a more rationalized institutional setup, stronger enforcement, and coalition-building with like-minded states in multilateral fora where European objectives are shared. Initiatives such as the Global Gateway can play a role in anchoring this external dimension of Europe's digital strategy.



02/

Second, the EU must build greater control over the technology layers of the digital stack by supporting European competitors in critical infrastructures such as cloud, compute, AI deployment, and semiconductor ecosystems and digital software applications, while diversifying partners and reducing one-sided dependencies. This must include effective means to channel capital and human talent (European and foreign) in these sectors.



03/

Third, Europe must strengthen its capacity to capture the benefits of the data-driven economy by enabling the emergence of European alternatives, promoting strategic catch-up to overcome legacy vulnerabilities, and reconceptualizing data not merely as a by-product of economic activity but as a strategic asset, the 5th factor of production, that underpins value creation and competitiveness.

04/

Fourth, the Union must enhance the modernity and adaptability of its critical infrastructures, particularly in the monetary and financial realm, by developing European safe assets, deepening and integrating capital markets, strengthening the euro's international role, and advancing projects such as the digital euro to reduce external vulnerabilities in payments and liquidity provision.

The stakes are high. The power of a regulatory-only European model is waning in a world where technological leadership and infrastructural control are becoming decisive sources of geopolitical strength. At risk is whether Europe becomes a complete vassal of the United States through structural dependence on defense and American platforms and digital ecosystems,[43] while remaining simultaneously vulnerable to China's control over critical chokepoints in the global technology value chain, especially in green tech.[44]

Dependencies will be difficult to untangle now. But later, they may become almost impossible to reverse. If Europe fails to align its normative ambitions with the material foundations of sovereignty, it risks becoming not a shaper of the digital order, but the battleground on which great power competition over the digital future is fought over.

> Ultimately, Europe's ability to sustain a new social contract in the digital age (the focus of the final work package of this project, which will start in 2026 and end 2027) will depend on whether it can secure the sovereignty, resilience, and strategic agency required to govern its technological transformation on its own terms.

REFERENCES

1 Lin, M., Chen, W., & Zhang, W. 2024. *The Era of Data as a Critical Production Factor.* In Big Data Finance in China (pp. 1-20). Singapore: Springer Nature Singapore. https://link.springer.com/chapter/10.1007/978-981-97-7981-9_1

2 Renda, A. 2023. *Data Policy: A Conceptual Framework. IE CGC.* https://static.ie.edu/CGC/Renda-Data_Policy_A_Conceptual_Framework-2023.pdf

3 Hobbs, C. 2020. *Europe's Digital Sovereignty: from Rulemaker to Superpower in the Age of US-China Rivalry. European Council on Foreign Relations.* https://ecfr.eu/wp-content/uploads/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf

4 Moerel, E.M.L, and Timmers, P. 2021. *Reflections on Digital Sovereignty. EU Cyber Direct, Research in Focus series 2021.* https://ssrn.com/abstract=3772777

5 Adler-Nissen, R., Eggeling, K. A. 2024. *The Discursive Striggle for Digital Sovereignty: Security, Economy, Rights and the Cloud Project Gaia-X. JCMS: Journal of Common Market Studies, 62: 993–1011.* https://doi.org/10.1111/jcms.13594.

6 European Parliamentary Research Service (EPRS). 2022. *EU strategic autonomy 2013-2023.* Brussels: European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733589/EPRS_BRI(2022)733589_EN.pdf

7 Australian Strategic Policy Institute (ASPI). 2024. *ASPI's Two-Decade Critical Technology Tracker.* Canberra: ASPI. https://www.aspi.org.au/report/aspis-two-decade-critical-technology-tracker

8 Blázquez-Navarro, I., Pujol, I., and Ruiz, V. 2025. *Defense in the Age of Deep Tech. Madrid: IE University—Center for the Governance of Change.* https://static.ie.edu/CGC/CGC_DefenseInAgeDeepTech.pdf

9 Gomes, A., Okano-Heijmans, M. and van den Wijngaard, J. 2025. *Beyond LEGO: the Need for EU-based Building Blocks of Technology. Madrid: IE University—Center for the Governance of Change.* https://www.ie.edu/cgc/publications/beyond-lego-the-need-for-eu-based-building-blocks-of-technology

10 Bria, F., Paul T., and Fausto G. 2025. *EuroStack—A European Alternative for Digital Sovereignty. Bertelsmann Stiftung.* https://www.euro-stack.info

11 Draghi, M. 2024. *The Future of European Competitiveness: A Competitiveness Strategy for Europe.* Brussels: European Commission. https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en

12 European Commission. 2024. *Communication on the Competitiveness Compass—Realising Europe's potential at home and abroad.* Brussels: European Commission. https://commission.europa.eu/document/download/10017eb1-4722-4333-add2-e0ed18105a34_en?filename=Communication_1.pdf

13 Jia, K., and S. Chen. 2022. "Global Digital Governance: Paradigm Shift and an Analytical Framework." *Global Public Policy and Governance* 2: 283–305. https://doi.org/10.1007/s43508-022-00047-w

14 Bradford, A. 2023. *Digital Empires. Oxford: Oxford University Press.*

15 Durand, C. 2020. *Technoféodalisme: Critique de l'économie numérique*. Paris: La Découverte.

16 UNCTAD (United Nations Conference on Trade and Development). 2021. *Digital Economy Report 2021. New York: United Nations.* https://unctad.org/page/digital-economy-report-2021

17 Schneider, I. 2025. "Reclaiming Digital Sovereignty: The EU's Role in the Geopolitics of Digital Governance." *Geopolitics of the Digital Era Paper 1. Madrid: IE University—Center for the Governance of Change*. https://static.ie.edu/CGC/CGC_ReclaimingDigitalSovereignty_PolicyPaper.pdf

18 Criddle, C. 2026. Microsoft warns that China is winning AI race outside the west. *Financial Times.* https://www.ft.com/content/f7a5b184-1fef-4f02-b957-4c2b07adf91f

19 Ganea, T. and Todorov, H. 2025. We Trained China's AI Researchers. Now We Risk Being Surpassed in AI Innovation. *The Standford Review.* https://stanfordreview.org/we-trained-chinas-ai-researchers-now-we-risk-being-surpassed-in-ai-innovation

20 Otero-Iglesias, M and Rodriguez, G. 2025. "From Brussels to Brasília: Regulatory Inspiration or Isolation?". *IE Insights*. https://www.ie.edu/insights/es/articulos/from-brussels-to-brasilia-regulatory-inspiration-or-isolation

21 Schneider, I. 2025. "Reclaiming Digital Sovereignty: The EU's Role in the Geopolitics of Digital Governance." *Geopolitics of the Digital Era Paper 1. Madrid: IE University—Center for the Governance of Change.* https://www.ie.edu/cgc/publications/reclaiming-digital-sovereignty-the-eus-role-in-the-geopolitics-of-digital-governance

22 White House. 2025. "Fact Sheet: President Donald J. Trump Issues Directive to Prevent the Unfair Exploitation of American Innovation." February 2025. https://www.whitehouse.gov/fact-sheets/2025/02/fact-sheet-president-donald-j-trump-issues-directive-to-prevent-the-unfair-exploitation-of-american-innovation

23 Gomes, A., Okano-Heijmans, M. and van den Wijngaard, J. 2025. *Beyond LEGO: the Need for EU-based Building Blocks of Technology.* Madrid: IE University—Center for the Governance of Change. https://www.ie.edu/cgc/publications/beyond-lego-the-need-for-eu-based-building-blocks-of-technology

24 European Parliament, *2023. The EU chips act: securing Europe's supply of semiconductors.* https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733596/EPRS_BRI(2022)733596_EN.pdf

25 Bertelsmann Stiftung, February 2025. *EuroStack—A European Alternative for Digital Sovereignty* (p. 66). https://www.euro-stack.info/docs/EuroStack_2025.pdf

26 Otero, M., Subacchi P., and Rodríguez, G.. 2025. *European Monetary Sovereignty in the Digital Age. Madrid: IE University—Center for the Governance of Change.* https://www.ie.edu/cgc/publications/european-monetary-sovereignty-in-the-digital-age/

27 Goodhart, Charles A. E., 1998. "The two concepts of money: implications for the analysis of optimal currency areas," *European Journal of Political Economy, Elsevier, vol. 14(3), pages 407-432, August. Otero-Iglesias, Miguel. 2014. Stateless Euro: The Euro Crisis and the Revenge of the Chartalist Theory of Money. Journal of Common Market Studies, pp. 1–16.*

28 Subacchi, P., 2023. *De-Risking the Global Financial System: Forging a "New Consensus", Policy Paper (New York: Friedrich-Ebert-Stiftung).*

29 Farrell, H. and Newman, A. L. 2023. *Underground Empire: How America Weaponized the World Economy. New York: Henry Holt and Co.*

30 Otero, M. and Rodriguez, G. 2025. "The Digital Euro: Let's Go Hybrid—but with a Public Backup." *IE Insights.* https://www.ie.edu/insights/articles/the-digital-euro-lets-go-hybrid-but-with-a-public-backup

31 EuropaWire. 2026. "European Payment Leaders Sign MoU to Create a Sovereign Pan-European Interoperable Payments Network", 2 February, 2026. https://news.europawire.eu/european-payment-leaders-sign-mou-to-create-a-sovereign-pan-european-interoperable-payments-network/eu-press-release/2026/02/02/15/34/11/168858/?amp

32 Torreblanca, J. I. and Giorgos, V. 2024. *Control-Alt-Deliver: A Digital Grand Strategy for the European Union.* European Council on Foreign Relations (ECFR). https://ecfr.eu/publication/control-alt-deliver-a-digital-grand-strategy-for-the-european-union/.

33 von Thun, M., G. Riekeles, y P. Kuzev. 2025. *Doubling Down, Not Backing Down: Defending the EU's Digital Sovereignty in the Trump Era.* Konrad-Adenauer-Stiftung. https://www.kas.de/documents/d/guest/doubling-down-not-backing-down.

34 European Commission. 2024. "Digital Partnerships." https://digital-strategy.ec.europa.eu/en/policies/partnerships

35 Hofmann, S. C., and Pawlak, P. 2024. *Harnessing Europe's Narrative Power to Shape the Digital Future. Washington, DC: Carnegie Endowment for International Peace.* https://carnegieendowment.org/research/2024/10/harnessing-europes-narrative-power-to-shape-the-digital-future

36 Gurumurthy, A. and Chami, N. 2024. "The Global Digital Compact Is Here: What Now for Civil Society?" *Bot Populi*, September 15, 2024. https://botpopuli.net/the-global-digital-compact-is-here-what-now-for-civil-society

37 European Commission. 2024. "EU-Latin America and Caribbean Digital Alliance." https://international-partnerships.ec.europa.eu/policies/global-gateway/eu-latin-america-and-caribbean-digital-alliance_en

38 Politico. 2024. "Focus Harder to Rival China's Vast Global Investment Plan, Brussels Is Told." April 23, 2024. https://www.politico.eu/article/focus-hard-rival-china-investment-plan-belt-road-initiative-brussels-eu-global-gateway; Torreblanca, J.I. & Vergi, G. 2024. *Control-Alt-Deliver: A Digital Grand Strategy for the European Union.* European Council on Foreign Relations (ECFR). https://ecfr.eu/publication/control-alt-deliver-a-digital-grand-strategy-for-the-european-union

39 Börzel, T. A., Krüsmann, V., Langbein, J., & Wu, L. 2023. *Colliding Scripts in Asia? Comparing China's Belt and Road Initiative and the EU Global Gateway Strategy. SCRIPTS Working Paper No. 34. Berlin: Cluster of Excellence "Contestations of the Liberal Script" (SCRIPTS).*

40 Arbouch, M., & Pelkes, A. 2024. *Bridging Gaps, Building Futures: Aligning the EU's Global Gateway and AFCFTA for Africa's Sustainable Integration.* European University Institute. https://cadmus.eui.eu/atmire/bitstream/1814/77757/1/STG_PP_2024_21.pdf

41 García de Viedma, D. 2026. "Pax Silica: alliances, frontier and markets in the geopolitics of the chip", 14 January 2026. Elcano Royal Institute. https://www.realinstitutoelcano.org/en/analyses/pax-silica-alliances-frontier-and-markets-in-the-geopolitics-of-the-chip

42 Del Amo, P. and Otero Iglesias, M. 2025. "The great challenge for Europe: balancing external security with internal social cohesion", 17 December 2025. Elcano Royal Institute. https://www.realinstitutoelcano.org/en/analyses/the-great-challenge-for-europe-balancing-external-security-with-internal-social-cohesion

43 Torreblanca, J. I. 2025. "Thrown under the omnibus: How the EU's digital deregulation fuels U.S. coercion", 3 December 2025. European Council on Foreign Relations (ECFR). https://ecfr.eu/article/thrown-under-the-omnibus-how-the-eus-digital-deregulation-fuels-us-coercion

44 Dellatte, J. 2025. "Cleantech: Reducing Europe's Strategic Dependence on China", Institute Montaigne, July. https://www.institutmontaigne.org/en/publications/cleantech-reducing-europes-strategic-dependence-china

IE UNIVERSITY

CENTER FOR THE GOVERNANCE OF CHANGE

WRITTEN BY:
Miguel Otero Iglesias and Gonzalo Rodríguez Gordo

RECOMMENDED CITATION:
Otero, Miguel, and Gonzalo Rodríguez (2026). *The Geopolitics of the Digital Revolution: Europe's Defining Test*. IE Center for the Governance of Change.

Photos: Unsplash, Shutterstock, Freepik.

Design: epoqstudio.com