THE FUTURE OF DIGITAL SOVEREIGNTY

TREND REPORT FALL 2025

CDTM
CENTER FOR
DIGITAL TECHNOLOGY
AND MANAGEMENT

Front Cover: Parthenon, Acropolis of Athens, Greece

The Acropolis, a fortress that has stood for over 2400 years, symbolizes resilience and sovereignty. As a cornerstone of European culture and democracy, it reflects the values Europe seeks to uphold in the digital age.

The Future of Digital Sovereignty

schwarz digits

Kindly supported by Schwarz Digits

Schwarz Digits is the digital division of Schwarz Group, one of the world's leading retail companies with the brands Lidl and Kaufland. As the central digital partner within the group, Schwarz Digits provides cutting-edge IT solutions, cloud services, and cybersecurity expertise. Its portfolio ranges from developing and operating the Schwarz Cloud, to ensuring data security, and driving digital innovation across retail and beyond.

With its deep commitment to digital sovereignty, Schwarz Digits helps businesses and institutions strengthen their independence in a globally interconnected and technologically competitive world. By combining entrepreneurial agility with large-scale digital infrastructure, Schwarz Digits enables secure, future-ready solutions that contribute to Europe's technological resilience.

Visit www.schwarz-digits.de for more information.

CDTM

A Project of the Center for Digital Technology and Management

The Center for Digital Technology and Management (CDTM) is a joint, interdisciplinary institution for education, research, and entrepreneurship of the Ludwig Maximilians-University (LMU) and the Technical University of Munich (TUM).

It offers the certificate program "Technology Management" for students from various backgrounds, which provides students with tools and knowledge at the intersection of business and digital technologies.

The entire trend report was written by CDTM students under the close guidance of research assistants.

Visit www.cdtm.com for more information.

TABLE OF CONTENTS

Dr. Alexander Schellong

Dr. Patricia Köpfer


PREFACE OF THE PROJECT PARTNER

Digital sovereignty is more than just a technological challenge – it encompasses political, economic, and societal dimensions. It addresses the urgent need for organizations, institutions, and governments to ensure control over their data, digital infrastructures, and value creation. This makes it a topic of high strategic relevance, especially in the context of global dependencies, regulatory frameworks, and the rapid rise of new digital technologies.

Partnering with CDTM on the seminar "The Future of Digital Sovereignty" was a natural choice. We were excited to collaborate with 26 interdisciplinary students who, under the guidance of an established framework, explored how digital sovereignty might evolve by 2040. Together, we investigated key questions: How can Europe strengthen its digital resilience? What role do technological innovations, political strategies, and economic ecosystems play? And how can businesses and institutions actively contribute to shaping a sovereign digital future?

The students analyzed a wide spectrum of trends – from geopolitical dynamics and societal shifts to emerging business models and disruptive technologies. The broad scope and complexity of this challenge required them to think holistically, bridging technological feasibility with ethical, legal, and cultural considerations. We were highly impressed by the depth of analysis, the creativity of ideas, and the professionalism shown throughout the seminar.

We would like to extend our sincere thanks to the students for their remarkable dedication and innovative spirit, which resulted in inspiring discussions and valuable insights. Our gratitude also goes to the seminar supervisors, whose guidance and close collaboration with us ensured a highly productive and enriching exchange.

Thank you all for seven intense weeks of research, exploration, and foresight – and for helping to define what digital sovereignty could mean for the decades ahead.

Dr. Alexander Schellong
Managing Director (GL), Member of the Executive Board

Dr. Patricia Köpfer
Cyber Education Manager

Vera Eger

Raunaq Jain


PREFACE OF THE EDITORS

> **"The future belongs to those who prepare for it today.**
>
> Malcolm X

From the phones in our pockets to the platforms that mediate civic debate and commerce, our lives increasingly unfold in digital spaces we neither design nor control. That is why digital sovereignty has become a defining issue of our time: the capacity of societies to shape their digital destiny. If we want technology to serve open markets, democratic values, and individual rights, we must build systems that are transparent, interoperable, and accountable. Open by default, not governed by gatekeepers.

At CDTM, our mission is to connect, educate, and empower the innovators of tomorrow. We equip our students with the tools and mindset to become responsible leaders who actively shape their future environments rather than merely respond to change.

This Trend Report is the outcome of the Trend Seminar within our interdisciplinary Technology Management program. Over seven intensive weeks, 26 students from fields including Architecture, Business, Psychology, Philosophy, Computer Science, and Engineering investigated "The Future of Digital Sovereignty". Working in interdisciplinary teams, they conducted rigorous trend research, developed forward-looking scenarios, and translated their insights into actionable product and service ideas as well as concrete business concepts by combining domain expertise with fresh perspectives and an entrepreneurial mindset.

We would like to thank everyone who contributed to making this CDTM Trend Report possible. We are especially grateful to Schwarz Digits for its support of this seminar. Our special thanks go to Alexander for the collaboration, insightful discussions, and steady feedback throughout the project. We also extend our gratitude to our lecturers, whose expertise and commitment were instrumental to the success of this report.

We hope these insights equip practitioners and policymakers alike to make timely, informed choices, as the architecture of digital sovereignty will shape not only innovation and competitiveness, but also the quality of everyday life for all of us.

In addition, we very much thank all our lecturers, who shared their knowledge and largely contributed to this project's success:

Aaron Defort (BCG)
Bernd Pichlmayer (FTGG Cyber)
Carmen Mas Machuca (University of the Bundeswehr Munich)
Elena Carlotta Herzog (CDTM)
Franz Waltenberger (CDTM)
Jakob Mayer (CDTM)
José Adrián Vega Vermehren (CDTM)
Kai Hermsen (DECAID)
Lisa Antonia Thiergart (CDTM)
Marie-Luise Wegg (NeoMINT)
Martin Hullin (Bertelsmann Stiftung)
Martin Wessel (CDTM)
Matthias Möller (CDTM)
Michael Fröhlich (CDTM)
Nadine Schmidt (CDTM)
Nina Feussner (Lakestar)
Oliver Schoppe (UVC)
Philipp Müller (DriveLock SE)
Ricardo Schaefer (Zone 2)
Sven-Christian Hörner (CDTM)
Tiemo von Hinckeldey (Valantic)
Zhenya Loginov (Accel)

Last but not least, we would like to thank the CDTM students of the Fall 2025 class. They put great energy and enthusiasm into this project, which made it a pleasure for us to supervise the course and coach the individual teams. Special thanks to the Heads of the editing, layout, sources, marketing, and QA teams (Malte, Katy, Danit, Hanano, and Karolina) for finalizing the report.

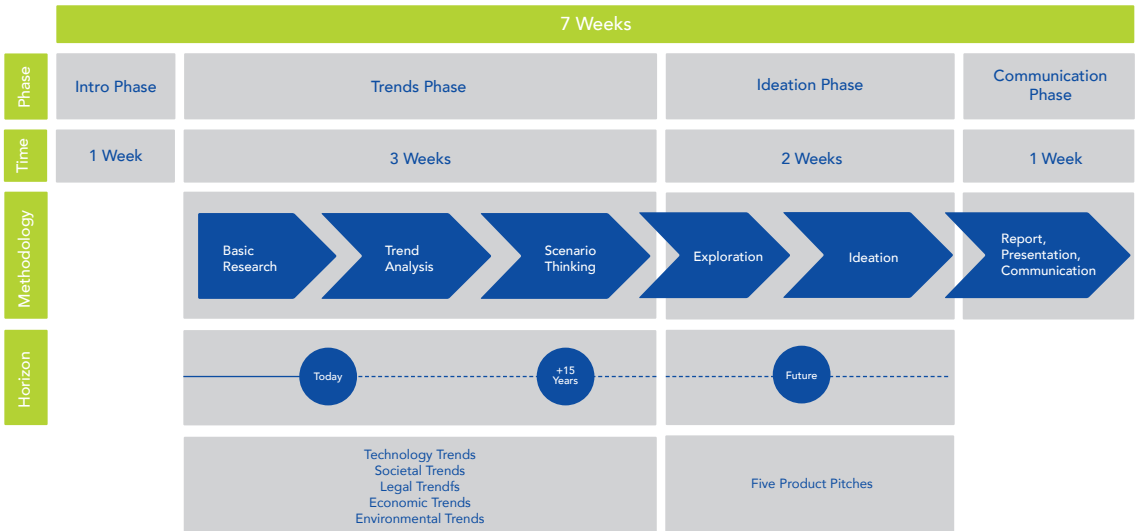
Vera Eger and Raunaq Jain

Center for Digital Technology and Management

METHODOLOGY

The objective of the Trend Seminar is to provide a methodological approach for diving into a specific subject or industry sector and contemplating its future trajectory. The seminar guides its participants through three phases of trend research: trend, exploration, and ideation. Following this approach, the seminar first analyzes current trends and developments using in-depth desk research, site visits, and interviews with leading experts to establish a shared industry understanding. Next, participants identify areas within the sector where problems and opportunities will likely arise. In the final seminar phase, the students generate future-proof business ideas for products and services, addressing the identified problems and opportunities.

Up to twenty-six students, supervised by two doctoral candidates, pursue the Trend Seminar for seven weeks full-time during their semester break. The sector and framing for the seminar is provided by project partners from within the industry, who share their expertise and feedback, acting as sparring partners to the participants. In each phase, interdisciplinary subteams are formed with students from business, technology, and other disciplines. This interdisciplinarity allows for novel ways of thinking and the development of non-obvious ideas as well as leveraging the students' professional and personal growth throughout the course.



During the introduction week, the participants are prepared for the intense trend research ahead. First and foremost, the students are introduced to the specific industry the seminar is diving into. Project partners and industry experts present past and current industry developments from their individual stakeholder perspectives, engaging in open discussions with the students. Additionally, interactive sessions teach trend research methodologies and refine the participants' communication and teamwork skills.

Following the introduction, the **trends phase** of the seminar covers desk research, expert interviews, and expert lectures, enabling the participants to dive deep into the topic at hand. During the expert interviews, students are empowered to pose specific questions to challenge their initial assumptions on how the industry will develop. Beyond that, site visits at the project partners' facilities complement the students' body of research and allow for further verification of their hypotheses. The derived trends are extrapolated 15 years into the future, providing a long-term perspective.

The first half of the **ideation phase** is about **exploring**. Future opportunities and problems are clustered into specific spaces based on the research done in the preceding phase. The students are reshuffled into new teams and explore these spaces by looking into existing start-ups and projects. Through interviews and discussions with industry experts, the teams validate their hypotheses to identify unmet needs and existing gaps in the industry landscape.

During the second half of the **ideation phase**, students brainstorm **business solutions** addressing the previously identified gaps. To facilitate the ideation process, the students are introduced to structured and unstructured ideation methods. This allows them to generate many ideas before consolidating them and building comprehensive business models. Finally, the research results and the business ideas are pitched to the project partners, industry stakeholders, and the general public.

LIST OF ABBREVIATIONS

AI
Artificial Intelligence

API
Application Programming Interface

ASAT
Anti-satellite

AWS
Amazon Web Services

AfD
Alternative für Deutschland

CAGR
Compound Annual Growth Rate

CISA
Cybersecurity and Infrastructure Security Agency

CRA
Cyber Resilience Act

CRM
Customer Relationship Management

CRMA
Critical Raw Materials Act

DDoS
Distributed Denial of Service

DORA
Digital Operational Resilience Act

EBIT
Earnings Before Interest and Taxes

EC
Edge Computing

ECC
Elliptic Curve Cryptography

EEA
European Environment Agency

EED
Energy Efficiency Directive

EIB
European Investment Bank

EIC
European Innovation Council

EOSC
European Open Science Cloud

EPI
European Payment Initiative

EPRS
European Parliamentary Research Service

ESA
European Space Agency

ESRS
European Sustainability Reporting Standards

EU
European Union

EU-CyCLONe
European Cyber Crisis Liaison Organisation Network

GDP
Gross Domestic Product

GDPR
General Data Protection Regulation

GPS
Global Positioning System

GPU
Graphics Processing Unit

ICT
Information and Communication Technologies

IP
Intellectual Property

IPCEI
Important Projects of Common European Interest

IPO
Initial Public Offering

IT
Information Technology

ITU
International Telecommunication Union

IoT
Internet of Things

KPI
Key Performance Indicator

LLM
Large Language Model

LMS
Learning Management System

ML
Machine Learning

MQTT
Message Queuing Telemetry Transport

Mt
Megatonnes

NATO
North Atlantic Treaty Organization

NIS2
EU Directive on Network and Information Security

NPU
Neural Processing Unit

O-RAN
Open Radio Access Network

OS
Operating System

OSS
Open-Source Software

PCI DSS
Payment Card Industry Data Security Standard

PPA
Power Purchase Agreement

PSD3
Payment Services Directive 3

PUE
Power Usage Effectiveness

R&D
Research & Development

RSA
Rivest-Shamir-Adleman

SME
Small and Medium-sized Enterprise

TWh
Terrawatt Hours

UNECE
United Nations Economic Commission for Europe

UNITAR
United Nations Institute for Training and Research

UPI
Unified Payments Interface

US
United States

VLA
Vision-language-action

WEEE
Waste Electrical and Electronic Equipment (Directive)

TRENDS

The following chapter lists current trends that have a strong influence on the development and long-term strategic orientation of *The Future of Digital Sovereignty*. In accordance with the Trends Phase methodology, trends and related driving forces are structured into five areas: technological trends, societal trends, legal trends, economic trends, and environmental trends.

TECHNOLOGICAL TRENDS

INFLUENCING THE FUTURE OF DIGITAL SOVEREIGNTY

Leveraging Edge Computing
Harnessing Advanced Robotics
Fostering Interoperability
Enhancing Cybersecurity
Securing Connectivity in the 6G Era

Atomium in Brussels, Belgium

Andriani Nikolaou 
Anjella Klaiber 
Danit Niwattananan 
Gjergj Kukaj 
Joseph Gawlik 
Nikolas Keller 

TECHNOLOGICAL TRENDS

Influencing the Future of Digital Sovereignty

Today technology underpins Europe's most vital infrastructure, and control over it has become a key source of geopolitical power. Nations leading in areas like semiconductors, cloud computing, and communication networks hold a significant strategic advantage in global competition. Europe remains reliant on foreign providers for its digital backbone, creating strategic vulnerabilities [1]. Digital sovereignty empowered by technological advancements is not a one-time achievement but a continuous process of building capabilities layer by layer. To preserve its sovereignty, Europe must continue to invest sustainably in critical technologies [2]. Over two decades, Europe's share of the global tech, media, and telecom market capitalization fell from 30% to 7%, representing an 8T EUR missed opportunity [3]. Europe also lags behind the United States (US) and China in eight of ten critical technologies, including artificial intelligence (AI), platforms, chips, and advanced computing [4]. Yet the building blocks for improvement exist: world-class research, a growing deep-tech ecosystem, and a tradition of industrial excellence. The share of European investment in deep tech has risen from 10% to 19% of global funding within four years, with strong momentum in AI, quantum, and robotics [5]. If Europe is able to transform these assets into scalable industrial capabilities, it will have a rare opportunity to reset its innovation engine and establish leadership in the next wave of technologies [6]. Five technological trends are particularly decisive for Europe's sovereignty. A key pillar is edge computing (EC), which brings processing closer to where data is generated, enabling real-time AI applications while keeping sensitive information under European control [7]. Building on this, advanced robotics translates digital intelligence into the physical world, boosting productivity, addressing labor shortages, and extending autonomy across industries [8]. For these infrastructures to interconnect, interoperability through open protocols is essential, allowing data and services to flow freely without dependence on dominant providers [9]. Moreover, advanced cybersecurity is necessary to protect critical data against evolving threats, including those posed by quantum computing [10]. Ultimately, 6G infrastructure will provide the future backbone, offering intelligent and secure connectivity that integrates people, devices, and industries on a global scale [11]. These trends share drivers of innovation, competitiveness, energy efficiency, and resilience, yet remain constrained by structural gaps. Europe leads in regulation and research but struggles to scale industrially. Dependencies on chips, batteries, and proprietary platforms persist across domains [12, 13]. Closing this "sovereignty gap" will require coordinated public-private investments, secure supply chains, and pan-European collaboration to ensure initiatives like Hexa-X, EuroQCI, or the Digital Decade Policy Program translate into lasting technological capabilities [1, 14, 15].

Looking forward, the trajectory of technological sovereignty will be determined by Europe's ability to build and integrate these technologies into resilient ecosystems. If Europe can effectively scale EC, robotics, interoperability, cybersecurity, and 6G, it can move from being primarily a regulator and consumer to a builder of sovereign digital infrastructures. Failure to do so risks deeper dependencies at a time of growing geopolitical and economic uncertainty.

LEVERAGING EDGE COMPUTING

Transforming the Internet of Things Through European Edge Nodes

EC is a distributed computing paradigm that moves computation closer to the data source, thereby reducing the need for large data transfers to centralized cloud servers [7]. Edge nodes, which are computing devices located near the data generation, enable this shift. They range from small Internet of Things (IoT) sensors and gateways to local servers capable of on-site analysis. This is crucial for maintaining the local control of sensitive data in industries such as healthcare, mobility, or defense. Processing data locally also reduces latency. EC combined with AI inference makes it possible for autonomous systems, for example, defense drones, robotics, and smart grids, to operate reliably without constant cloud connection. These systems cannot rely on distant cloud servers, as they require instant decisions for safety and reliability [7]. Building on this, IoT and robotics are the primary beneficiaries, since they generate vast amounts of data and demand both fast processing and secure handling. Recognizing this potential, the European Commission is investing heavily in EC and IoT, viewing them as central to the digitization of the economy [16].

Facts

- Edge AI enhances technologies in autonomous vehicles, healthcare, IoT, drones, and security systems [17].
- In 2024, 70.9% of EU citizens used IoT devices, indicating strong adoption potential, especially in consumer IoT [18].
- Integrating EC into hybrid cloud-edge architectures can cut energy use by 19–28% compared to centralized setups and can help to offset the growing energy demands of digital infrastructure [19].
- Strategic European initiatives, such as 8ra, are pursuing a digital infrastructure that relies on multiple providers and edge nodes designed to counteract the dependency on American hyperscalers by building a hybrid cloud [20].

Key Drivers

- EC is projected to grow from 564.6B USD in 2025 to over 5T USD by 2034 with a Compound Annual Growth Rate (CAGR) of 28%. Industrial IoT, which accounts for over 33% of market revenue, is a major driver of this growth [21].
- The EU has committed to deploying 10,000 climate-neutral, highly secure edge nodes by 2030 under the Digital Decade Policy Programme [22].
- Open IoT standards such as Message Queuing Telemetry Transport (MQTT) and European open-source frameworks like FIWARE make IoT easier by reducing integration complexity and by supporting deployments that are secure, scalable, and adaptable [23].

Challenges

- Non-European computing services and AI models dominate the European market [1]. Achieving independence throughout the value chain of edge AI, requires either relying on less advanced open-source models or investing heavily in proprietary models [24].
- Edge devices have limited computing power and strict low-latency requirements. Current cloud orchestration frameworks, such as Kubernetes, were designed for centralized data centers and do not meet the criteria for efficient task scheduling, workload distribution, and resource management in highly distributed edge environments [25].

Impact on European Digital Sovereignty

The European Commission acknowledges that ensuring Europe's digital autonomy in information and communication technologies (ICT) requires strong computing capacity [16]. Many data-intensive applications, including Extended Reality and Digital Twins, rely on EC and benefit from local control over sensitive industrial and consumer data [7]. Looking ahead, many technological trends, including AI-powered robotics and drones, will depend on the capabilities of edge infrastructure. As EC matures, it will become an essential pillar of Europe's digital sovereignty, transforming entire industries by enabling more intelligent factories, autonomous mobility systems, and a more digital society.

HARNESSING ADVANCED ROBOTICS

Driving Productivity with AI-Powered Robots for Novel Applications

The integration of AI and robotics is reshaping economies. Advanced robotics combines AI and Machine Learning (ML) methods such as computer vision, reinforcement learning, and large language models (LLMs) with robotic systems to perform tasks with greater precision, adaptability, and autonomy compared to traditional robots [26]. The global operational stock of industrial robots has been growing at an average annual rate of 12%. In 2023, Europe held a share of ~18%, ranking second after China [8]. With this intelligence, robotic applications are rapidly expanding beyond manufacturing [26]. Robots boost productivity and create safer workplaces by collaborating seamlessly with humans through advanced sensing and safety features [27]. Autonomous mobile robots operate independently in dynamic environments, optimizing logistics and material handling with minimal oversight. Furthermore, humanoid robots, equipped with sensors and cognitive abilities, can converse and assist with daily, repetitive tasks [28].

Facts

- Robots are becoming smarter and are increasingly used outside traditional manufacturing, with usage growing by 20–35% annually in logistics, hospitality, and agriculture [26].
- Chinese companies predominantly manufacture the necessary hardware for intelligent robots. In contrast, the production of advanced AI chips that enable their capabilities is dominated by US companies and Taiwanese manufacturers [13].
- Neural processing units (NPUs) are experiencing growing adoption for running AI predictions in robotic edge devices. They are being integrated more closely into chip processors, with the market size projected to grow at a CAGR of 18.95% from 2025 to 2033 [29].

Key Drivers

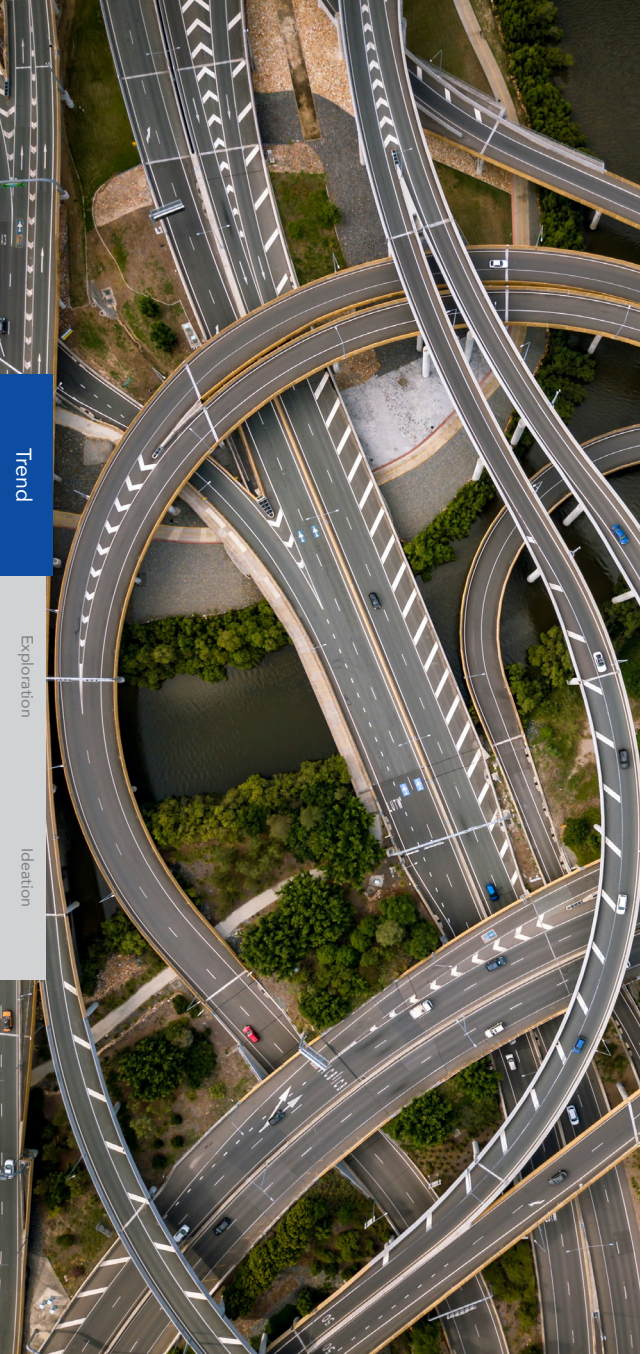
- Over the last 30 years, labor costs in the EU have increased by 40%, while labor shortages have emerged. At the same time, production costs incurred by robots have declined by 20%, making the technology more accessible and economically viable [30].
- AI and ML methods enable robots to perceive environments more effectively, perform smarter adaptive tasks, and facilitate more natural human-robot interaction [31].
- NPUs excel in specific neural network tasks while providing lower latency and power consumption. This is a critical advantage for robotics, where decisions must be made in real time and devices often run on battery power [32].

Challenges

- There is insufficient data to train foundational models to perform complex tasks and perform reliably on novel situations [26]. While this is partially addressed by supplementing synthetic simulation data, the transfer to the real world remains challenging [33].
- The complete automation of robots as AI agents using visual-language-action (VLA) models remains unreliable compared to logic-based programming, which prevents them from being deployed safely in unpredictable real-world situations [34].
- Mobile robotic platforms face hardware limitations, which limit their operation duration or ability to perform more complex computations for complicated tasks [35, 36].

Impact on European Digital Sovereignty

The adoption of advanced robotics is central to Europe's industrial competitiveness and labor shortage problem. Still, the continent's reliance on non-European suppliers for critical hardware and proprietary data generation software creates strategic vulnerabilities. This reliance risks limiting Europe's autonomy in scaling advanced robotics across industries. Strengthening domestic production capabilities and fostering innovation and collaboration in the components mentioned, including key technologies such as NPUs, will therefore be crucial to ensuring that Europe not only benefits from robotics-driven productivity gains but also preserves its technological sovereignty in an increasingly volatile global economy.



FOSTERING INTER-OPERABILITY

Creating a Sovereign Digital Ecosystem Through Software Interoperability

The European Union is striving to strengthen digital interoperability by leveraging open–source solutions to dismantle proprietary silos, which create closed ecosystems that trap user data and limit competition [37]. While interoperability can be fostered through closed-source methods, such exclusive approaches allow only limited connections and often maintain dependence on a single vendor's infrastructure. By contrast, open protocols and open-source reference implementations allow any provider to adopt and extend the standard, creating a level playing field where users can switch providers without losing access to their data or functionality. This lowers switching costs, prevents market lock-in, and encourages competition based on service quality rather than ecosystem control [37]. The EU's focus on interoperability is therefore not merely technical but strategic: it is a deliberate response to the market dominance of large technology companies, designed to redistribute power, stimulate innovation, and make the European digital ecosystem more resilient [37].

Facts

- Companies estimate their software costs would be 3.5 times higher without open-source alternatives [38].
- The global open-source software (OSS) market, a key driver of interoperability, was estimated at 25.03B USD in 2022 and is projected to reach 83.87B USD by 2030, growing at a CAGR of 16.9% through 2030 [39].
- The global Application Programming Interface (API) management market is projected to grow from 8.86B USD in 2025 to 19.28B USD by 2030, at a CAGR of 16.8%, reflecting the shift in enterprise solutions [40].
- Public investment in open-source infrastructure is rising. Germany established a Sovereign Tech Fund in 2022 with a budget of 17M EUR to support critical open-source projects [41].

Key Drivers

- The success of open solutions is demonstrated internationally by initiatives such as India's Unified Payments Interface (UPI), which utilizes an open protocol to facilitate instant, direct bank-to-bank payments across various applications [42].
- Cost savings and simplified service integration are driving industrial adoption of OSS, with OSS constituting 70–80% of any given piece of modern software [43].
- Institutional support for OSS is growing in Europe. The European Data Protection Supervisor has launched pilot projects using decentralized alternatives to centralized platforms, such as Mastodon and PeerTube, to enable users to freely move their data and identity [44].

Challenges

- Established platforms benefit from strong network effects, which make it difficult for new interoperable alternatives to gain traction. The scale of this is clearly reflected in the user numbers, as e.g., Mastodon has about 255,000 monthly active users, while Instagram has over 2B [45, 46].
- Organizations resist sharing their data openly due to concerns about power and control, fearing a loss of strategic advantage. This resistance reinforces data lock-in and slows the adoption of interoperable solutions [47].
- Content moderation and data security are difficult to implement consistently across interoperable networks. Addressing these issues requires new governance and funding models [48].

Impact on European Digital Sovereignty

Interoperability enabled by open solutions strengthens the EU's digital sovereignty by lowering entry barriers, fostering innovation among European companies, and reducing the market power of dominant technology platforms [9, 47]. It provides users with greater control by enabling seamless data portability between services, preventing vendor lock-in, and upholding the principles of the General Data Protection Regulation (GDPR) [37]. Europe will only achieve true digital sovereignty if it actively develops the capabilities, platforms, and infrastructures that are enabled by open protocols and interoperability [2].

ENHANCING CYBER-SECURITY

Ensuring Long-Term Data Resilience Through Post-Quantum Security

As quantum computing advances, many of today's widely used cryptographic methods will eventually become obsolete. This development poses a risk, particularly in sectors that handle sensitive data, such as finance, defense, and healthcare. In 2023, the latter experienced a significant increase in Distributed Denial-of-Service (DDoS) attacks, which attempt to overwhelm networks with high traffic, resulting in nearly 100 attacks per day [49]. To counter this, Europe is investing heavily in long-term cyber resilience. The EuroQCI project aims to establish a quantum-secure communication network across all EU member states by 2027, utilizing fiber cables and satellites to distribute encryption keys, thereby enhancing security. [15]. Meanwhile, organizations are preparing to adopt post-quantum standards [10], with policymakers stressing the need for agility in cybersecurity, ensuring that systems can transition smoothly as new protections emerge [10, 50]. To ensure Europe's data remains secure in the long term, it is crucial to begin developing and implementing post-quantum technologies today [10].

Facts

- The European post-quantum cryptography market was valued at 162.8M USD in 2024 and is expected to grow annually by 42.16%, reaching 5.5B USD by 2034 [51].
- Global cyberattacks increased by 21% year-over-year from 2024 to 2025 [52].
- The healthcare sector experienced a surge in attacks in 2023, with nearly 100 attacks per day, exposing it as one of the most vulnerable sectors [49].
- Quantum computers could potentially break standard encryption methods, such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC), which rely on mathematical complexity for secure key exchange [53].

Key Drivers

- The Network and Information Security Directive (NIS) 1 and 2 are EU-wide regulations designed to strengthen cybersecurity across critical sectors and set baseline security requirements for operators of essential and digital services [54].
- Europe has the capabilities to develop new quantum technologies, exemplified by Anton Zeilinger. The Austrian physicist won the 2022 Nobel Prize for pioneering work in quantum entanglement, which has inspired research in quantum communication [55, 56].
- Policymakers emphasize the need for systems to transition seamlessly to post-quantum security. All EU member states are expected to begin this shift by the end of 2026 [50].

Challenges

- In 2022, the EU faced a shortage of 260,000–500,000 cybersecurity professionals, out of an estimated need of ~883,000, significantly hindering the deployment of advanced technologies [57].
- As of July 2025, only 14 out of 27 EU member states had incorporated the NIS2 directive into national law [58].
- Integrating advanced solutions into legacy infrastructure is costly and technically challenging. Industrial systems often cannot adapt to post-quantum models without major redesign [59].
- Europe's diverse vendor landscape and evolving certification schemes create integration and compliance burdens, slowing adoption [60].

Impact European Digital Sovereignty

The rise of quantum computing and the shift toward post-quantum cryptography have significant implications for Europe's digital sovereignty. Reliance on traditional cryptographic standards could expose sensitive data to external control or compromise its integrity. Europe can maintain control over its critical data flows and communications by deploying modern quantum-secure infrastructure and adopting post-quantum algorithms. Furthermore, strengthening crypto-agility ensures that Europe can rapidly adapt to emerging threats without relying on external actors, thereby safeguarding its long-term strategic autonomy in finance, healthcare, defense, and other critical sectors.

SECURING CONNECTIVITY IN THE 6G ERA

Advancing Europe's Path to Resilient Networks Through 6G

Positioned as the next standard for global communication, 6G is designed to integrate mobile and satellite-based internet networks into a unified, intelligent infrastructure. Within 6G, devices will seamlessly switch to the best available connection, extending reliable coverage to previously uncovered areas. This "network of networks" enables real-time coordination of billions of endpoints [11]. Future applications include autonomous cars exchanging updates within milliseconds to avoid collisions or thousands of sensors reporting continuously [61]. This growing data exchange makes high-throughput data transmission and thus new frequency bands essential [62]. For this to work, EC nodes will enable local AI to manage the network with near-zero latency [12]. The strategic importance of 6G lies in determining who sets the global standards and holds the key patents, as this will shape the technologies adopted worldwide and dictate where value and influence accrue. Europe's experience with Huawei during the 5G rollout illustrates the risks: while Huawei offered cost-effective and advanced equipment, its dominant role triggered widespread security concerns, leading several countries to restrict or phase out its gear from critical networks. The rollout of 6G, therefore, is a critical chance to make our critical infrastructure more sovereign and reduce dependencies [61, 62].

Facts

- The first commercial 6G networks are expected to be available around the early 2030s [63].
- Europe has committed at least 1.8B EUR to 6G research, with member countries developing local programs that contribute to the broader European agenda [64, 65].
- There is intense global competition, with China filing 40.3% of 6G patents, the US 35.2%, and Europe accounting for only 8.9% [66].
- The EU flagship programs Hexa-X and Hexa-X-II, led by Nokia and Ericsson with over 40 partners, are researching and developing the first 6G concepts to secure the European influence in global standard-setting [11, 67].

Key Drivers

- The need for strategic autonomy pushes Europe to invest in 6G, as the control over standard-setting not only defines the global technological landscape but also determines who collects royalties [62, 68].
- The rise of digital media, Industry 4.0, and real-time AI is driving latency and throughput demands that far exceed the abilities of 5G [61, 62].
- Rising cyber and military threats make secure, resilient networks indispensable, since future hospitals, energy grids, and armed forces will depend on uninterrupted and tamper-proof connectivity [11, 69].

Challenges

- Europe depends on highly specialized chips, rare earths, and patented processes from abroad, creating supply chain and licensing vulnerabilities for the 6G infrastructure [12].
- Current hardware cannot efficiently process the extreme 6G bandwidths. Handling vastly larger data volumes requires new chip architectures, faster converters, and energy-efficient processors. Without these breakthroughs, power consumption will rise to unsustainable levels [70].
- The high frequencies used in 6G have very short ranges and are easily blocked by obstacles. Overcoming this requires new hardware, such as advanced antenna technologies [70].

Impact on European Digital Sovereignty

6G will be decisive for Europe's sovereignty as it determines who owns the licensing of future communication. By shaping standards and securing patents, Europe can avoid dependence on foreign technologies that dictate costs, technical frameworks, and security protocols. Without secure, always-available networks, Europe risks disruptions to vital services, making robust, tamper-resistant connectivity a cornerstone of sovereignty. Therefore, building knowledge through European-led programs like Hexa-X is essential to ensure that future digital infrastructures reflect European priorities of trust, security, and autonomy.

SOCIETAL TRENDS

INFLUENCING THE FUTURE OF DIGITAL SOVEREIGNTY

Rising Demand for European Digital Tech
Intensifying Tech Talent War
Widening Digital Literacy Gap
Building European Big Tech Alternatives
Reconciling Europe's Paradox of Identity

Sassi di Matera in Basilicata, Italy

Estelle Kulow 
Hanano Shiga 
Joe Lammers 
Malte Oberhoff 
Salan Isaqzoi 

SOCIETAL TRENDS

Influencing the Future of Digital Sovereignty

Digital sovereignty is usually described in terms of policies, technologies, and regulations designed to limit dependence on foreign providers. However, focusing only on these structural aspects overlooks a deeper reality: sovereignty in the digital age is ultimately shaped within society itself. It unfolds through three interconnected dimensions: consumer choices, innovation capacity, and collective identity. These dimensions determine whether citizens, firms, and institutions can create, adopt, and sustain European digital alternatives. Without societal demand, practical skills, and shared legitimacy, any measures will have limited impact and remain largely symbolic.

Consumer choices shape the market for European digital products, as Europeans increasingly value privacy, fairness, and transparency over raw functionality, driving demand for trusted alternatives [71]. Yet adoption is constrained by price sensitivity and entrenched vendor lock-in, while foreign providers often adapt to local rules without ceding control [72, 73]. European values may guide consumer preferences, but economic and structural barriers frequently prevent them from translating into substantial market share or lasting competitive advantage for European alternatives.

Moreover, innovation capacity determines whether Europe can convert demand into supply. Digital technologies evolve faster than people's ability to use them, producing gaps in basic digital literacy and advanced Information and Communication Technology (ICT) skills [74, 75]. Europe trains world-class AI specialists at competitive per-capita rates, yet many leave for more lucrative positions abroad [76, 77]. These shortfalls, ranging from insufficient baseline skills to persistent "brain drain," both blunt consumer agency and limit the region's capacity to design, scale, and secure homegrown technologies. Without closing both gaps, European supply cannot reliably meet European demand [78].

Ultimately, collective identity shapes both consumption and political will. Although trust in EU institutions is rising and a sense of European identity is strengthening, national attachments remain stronger for most citizens [79, 80, 81]. Many people adopt hybrid positions, combining national pride with support for European cooperation, and leaders often reflect this duality. That ambivalence can mobilize broad coalitions for shared projects, but it also creates openings for Eurosceptic narratives that undermine long-term commitment to collective solutions [82]. Political legitimacy, therefore, determines whether social preferences translate into sustained public policy and private investment.

These dimensions are tightly interlinked and mutually reinforcing. Consumer choices generate demand signals. Innovation capacities determine whether those signals result in usable, secure products. Collective identity underpins the social consent required for coordinated public action and investment. Left unaddressed, the combination of price sensitivity, skills shortfalls, and contested identities risks a counterproductive equilibrium: Europe trains talent that benefits foreign competitors, regulates systems it does not control, and struggles to align consumer preferences with durable political and industrial strategies. Achieving digital sovereignty, therefore, requires integrated approaches that strengthen market conditions, upskill populations, and build political consensus so societal demand can be converted into resilient European alternatives [71, 80, 83].

RISING DEMAND FOR EUROPEAN DIGITAL TECH

Choosing European Digital Platforms for Trusted Solutions

Europeans' decision criteria for digital products are increasingly shifting from pure functionality toward trust, transparency, and alignment with core European values such as privacy, fairness, and democracy [71]. Moreover, rising concerns about data privacy, repeated cybersecurity incidents, and discontent with the dominance of US and Chinese platforms are accelerating the search for homegrown alternatives [72]. Consequently, European providers that embed European values into their services, such as ProtonMail and Ecosia, are gaining traction [84, 85]. This growth, fueled by European demand, is evident in both consumer and enterprise markets as executives increasingly view digital sovereignty as a strategic necessity to reduce reliance on foreign infrastructure and mitigate the pricing power of non-European suppliers [86]. Additionally, grassroots initiatives such as the Reddit community "r/BuyFromEU" and apps like "GoEuropean" raise awareness of product origins and connect consumers directly with European alternatives [87, 88]. This suggests that momentum is driven not only by regulatory or corporate forces, but also by cultural influences and bottom-up consumer choices.

Facts

- Europeans show a strong willingness to replace US products with a median substitution score of 80 out of 100 [72].
- European digital platforms, such as ProtonMail and Ecosia, have reported strong growth, with the latter increasing by 19% from 2024 to 2025 [84, 85].
- Alongside initiatives like Deutsche Telekom's "Open Telekom Cloud," the launch of Microsoft's EU sovereign cloud shows that non-European providers are also adapting [89].
- Hybrid cloud adoption is accelerating, as 66% of European firms now consider the combination of on-premise compute and public cloud services essential for business success. Adoption rates are expected to double by 2026 [90].

Key Drivers

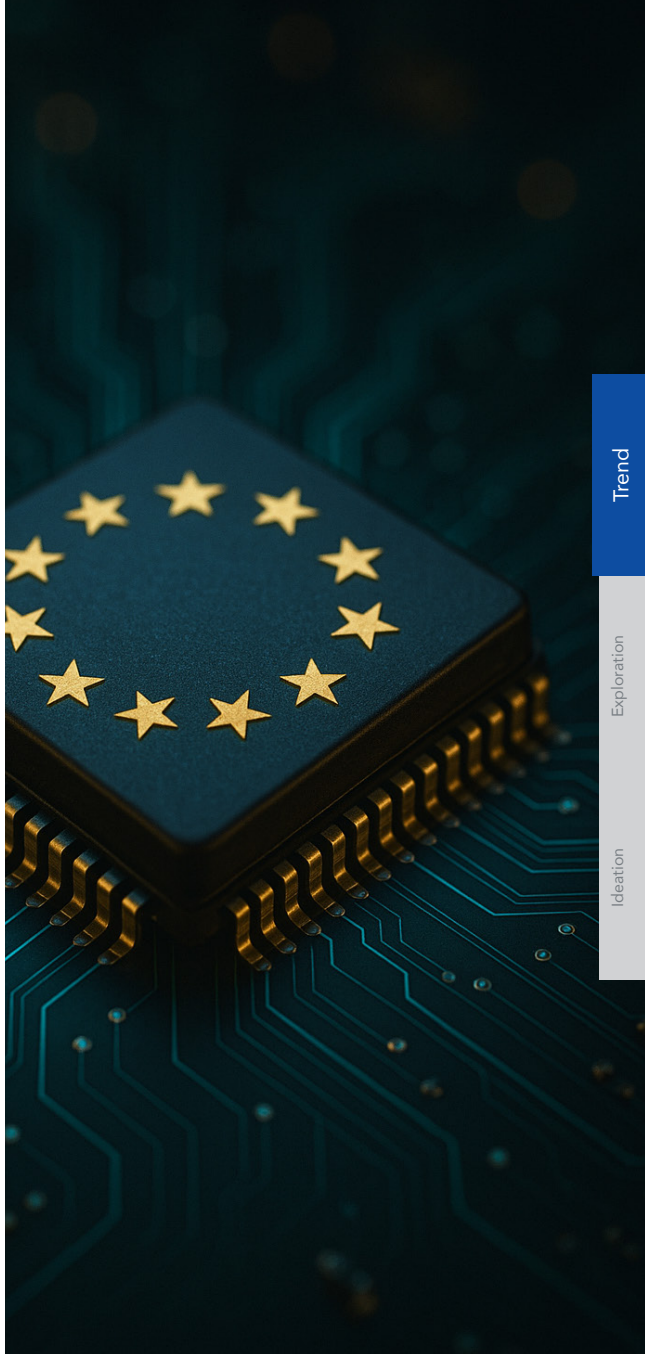
- Repeated misconduct by Big Tech and cyberattacks are boosting demand for sovereign, secure technology. 82% of Europeans support clear rules for digital technologies, and 84% say AI must be carefully managed to protect privacy and ensure transparency [91].
- Control over proprietary data is emerging as a decisive competitive advantage, empowering companies to reduce dependence on external providers and strengthen their market position [92].
- Executives are increasingly alert about vendor lock-in, a concern reinforced by recent price hikes from major tech providers, such as Microsoft's 5–25% increase in subscription costs [56].

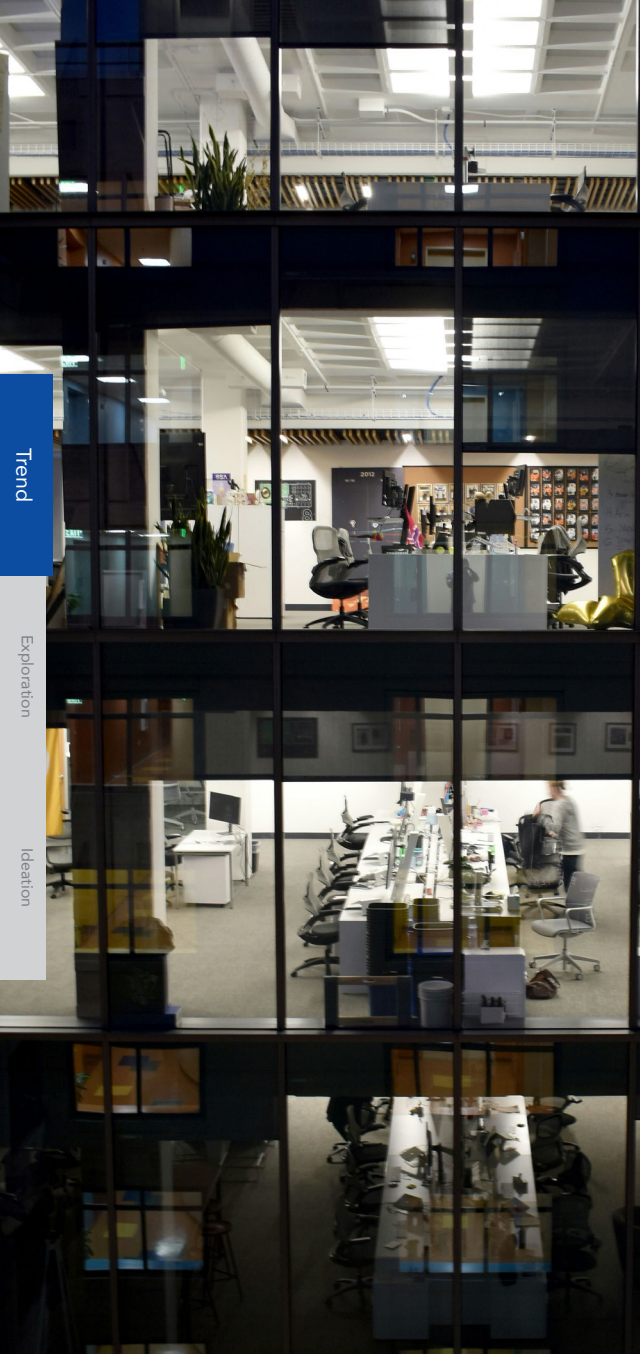
Challenges

- Price sensitivity limits mass adoption at both the company and consumer levels. While many low-income households support the idea of "Made in Europe," they are often hesitant to pay a premium for it. On the business side, companies require economically competitive alternatives. However, Europe-based providers often lack the scale and cost efficiency of their US competitors [72].
- Vendor lock-in, caused by multi-year cloud contracts, deeply integrated infrastructure, and high switching costs, limits the flexibility of European firms. This makes it difficult for them to move away from US hyperscalers, which hold 70% of the European cloud market [56, 73].

Impact on European Digital Sovereignty

The rising demand for trusted European digital products strengthens Europe's ability to regain control of its digital infrastructure. Although progress is hindered by vendor lock-in and a lack of competitive European alternatives, each shift away from US or Chinese platforms reduces their pricing power and data dominance. These shifts show that sovereignty is not only a regulatory ambition but a market reality driven by bottom-up demand. By embedding privacy, fairness, and transparency into everyday services, European companies can turn digital sovereignty into a competitive advantage rooted in cultural alignment and consumer trust.





INTENSIFYING TECH TALENT WAR

Competing for Global AI Talent as a Strategic Asset

In today's digital economy, demand for software engineers, data scientists, and AI specialists is growing faster than ever, as companies increasingly rely on technology to compete. These ICT specialists form the backbone of Europe's digital transition [78]. Within the ICT sector, AI talent has emerged as the most contested segment, driven by rapid technological advances and its strategic importance for economic competitiveness. While Europe produces a high number of AI specialists, it faces challenges in retaining them, as many are drawn to more lucrative opportunities in countries such as the US or China [83]. In response to the strong pull of foreign firms, the EU is expanding investments and initiatives such as easing immigration rules for skilled workers, fostering local expertise, and leveraging strengths in research and regulation [93, 94]. However, without significantly greater scale, these efforts risk being eclipsed by the financial capital and recruitment capacity of US and Chinese tech giants [77]. Simultaneously, political shifts and targeted initiatives, along with the AI-driven automation of junior roles, are intensifying competition for senior talent [83].

Facts

- AI specialists are in high demand, with 75% of employers in the EU reporting shortages in 2023 [95].
- Europe trains AI talent at globally competitive levels, 30% more experts per capita than the US and nearly three times that of China, yet many leave for jobs abroad [76, 83].
- Differences in pay highlight the challenge as senior AI scientists in Europe earn far less than their US counterparts, with, for example, Meta senior scientists in the US making up to 20M USD and OpenAI researchers receiving signing bonuses of 100M USD [77, 96].
- Following recent funding cuts in the US, 75% of researchers consider relocating to Europe or Canada, creating a unique opportunity that Europe tries to capture with initiatives such as "Choose Europe" [94, 97].

Key Drivers

- Despite declining software engineer salaries, specialized skills in AI, cloud computing, and cybersecurity remain in high demand, creating selective talent shortages [83].
- Beyond pay, factors such as strong universities, English-language proficiency, and vibrant tech ecosystems shape a region's attractiveness to AI talent [83].
- US tech companies influence AI education and talent development by offering free learning resources, which both widen training gaps across regions and help them attract the world's top professionals [98, 99].

Challenges

- Attracting global talent is constrained by fragmented regulations, complex visa procedures, and non-English-speaking workplaces, which limit Europe's pull compared to larger English-speaking ecosystems [83].
- Retaining top specialists is equally difficult, as higher salaries, resources, and prestige abroad continue to draw them away. Highly skilled professionals also gravitate toward established clusters of excellence, reinforcing the dominance of US hubs and creating a self-perpetuating cycle that weakens Europe's ability to scale its own ecosystems [83, 100].

Impact on European Digital Sovereignty

When Europe not only trains but also successfully attracts and retains tech talent, it builds a more resilient and self-sustaining digital ecosystem, constituting a key pillar of digital sovereignty. Without a skilled workforce, innovation stagnates and Europe risks ceding control over the design, deployment, and governance of critical technologies such as AI, thereby becoming dependent on foreign solutions. In this context, skilled talent is the foundation for developing competitive Europe-based digital alternatives with comparable or superior capabilities. Securing digital sovereignty, therefore, hinges on Europe's ability to attract, retain, and effectively deploy this expertise.

WIDENING DIGITAL LITERACY GAP

Bridging Knowledge Gaps as Technological Progress Outpaces Learning

Digital technologies are evolving faster than people's ability to use them effectively, leading to a digital skills shortfall [74]. Among European countries, Germany's digital literacy is below average with most other countries lagging behind their goals [101]. International assessments show that many students remain stuck at basic proficiency levels, while older generations face uneven access to upskilling opportunities, depending on factors such as region, occupation, and socio-economic background [102]. Even Generations Z and Alpha, despite high technology adoption rates, often lack advanced technical skills going beyond mere consumption [103].
However, these skills are essential both to drive innovation for competitive European alternatives and to implement cybersecurity measures needed to protect Europe's infrastructure from foreign interference. Without a strong foundation ranging from coding to advanced AI expertise, Europe risks dependence on external technologies and talent [78]. Closing this knowledge gap requires coordinated efforts from schools, employers, and governments to build a workforce capable of meeting the demands of digital sovereignty.

Facts

- In the US, close to 60% of adults struggle with basic digital tasks, while EU performance varies widely: Nordic countries like Finland outperform the US, but several EU states show declining skills [101, 104].
- Finland has treated digital literacy as a "civic competence" since the 1970s by embedding it in school curricula. This long-term commitment has positioned the country as second in the EU, with 82% of the population having at least basic digital skills [75].
- Digital skills are increasingly essential for employment, with 90% of jobs now requiring at least basic digital competencies [105].

Key Drivers

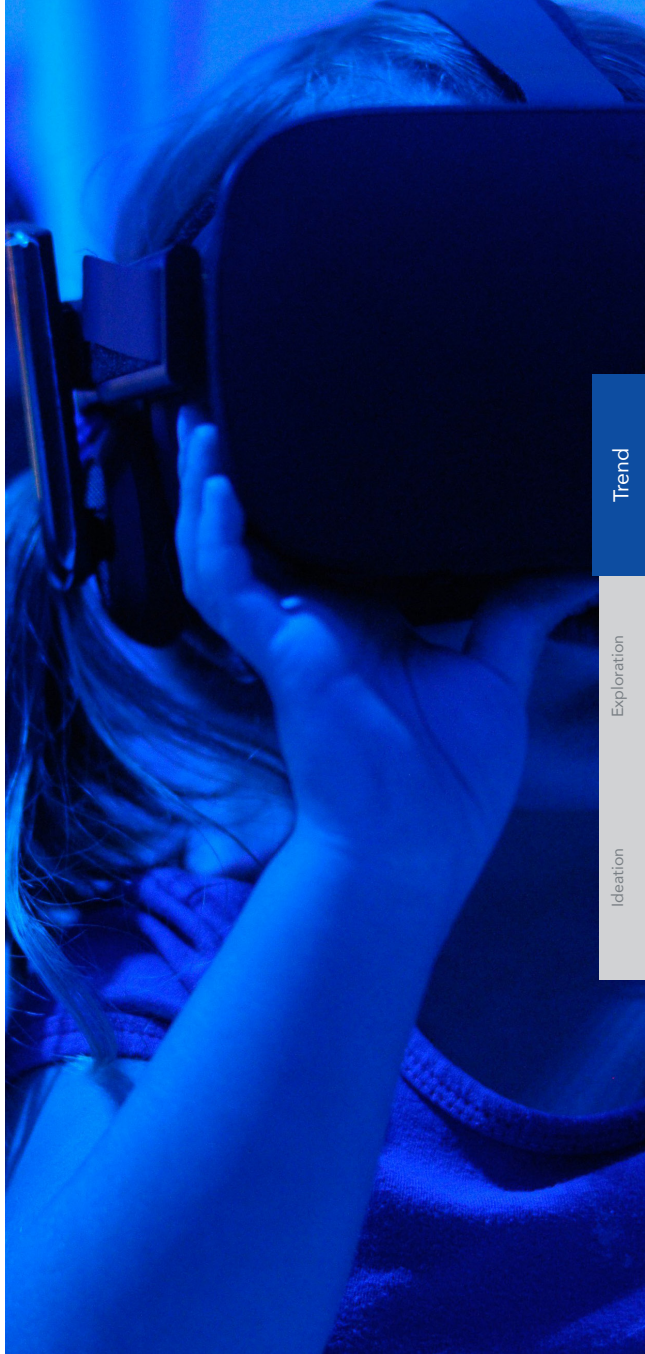
- Digital skills in the EU are strongly tied to education. 80% of people with higher education have at least basic skills, compared with 34% among those with low or no formal education. A lack of trained staff and rapid innovation, making lower education curricula difficult to standardize, drive this dynamic further [75, 78].
- The value of digital skills lies in their application, yet widespread risk aversion and fear of failure often hinder the adoption of new technologies, thus diminishing the true impact of digital literacy [104].
- Digital skills now shape who gets hired, how much they earn, and whether they can get promoted [105].

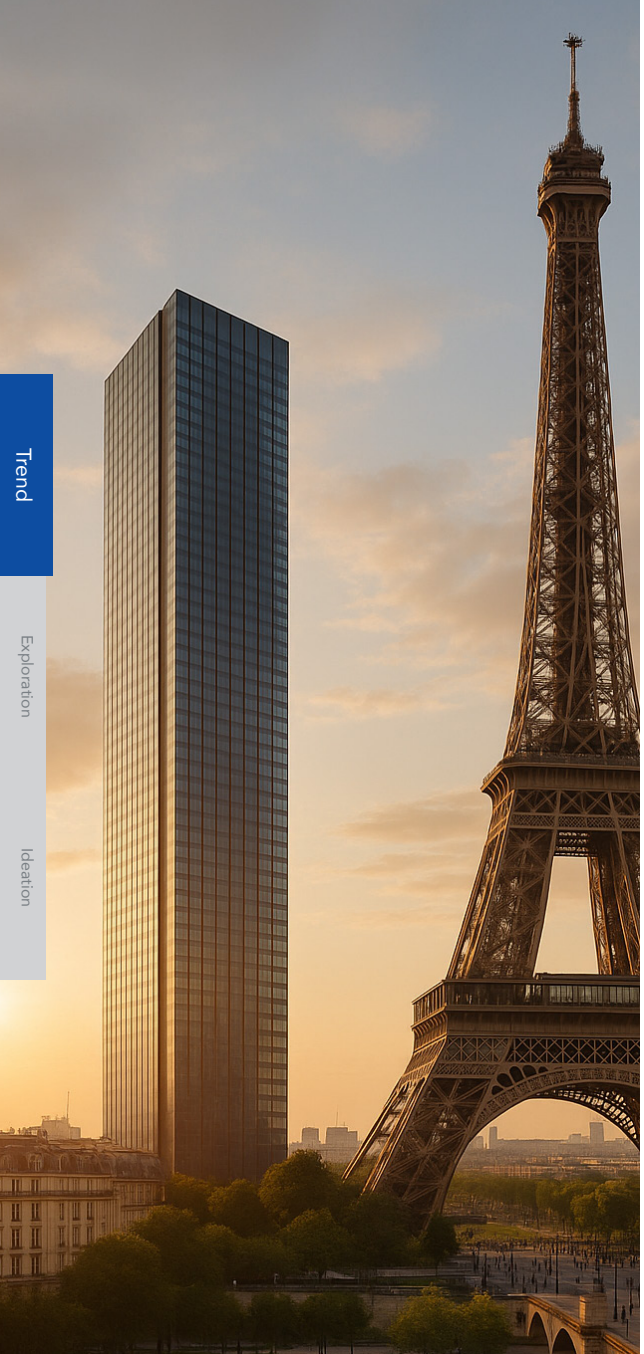
Challenges

- Weak information literacy and critical thinking increase vulnerability to manipulative content, and AI tools amplify these risks. Protecting minors is especially difficult given their high digital adoption. The Digital Services Acts' (DSA) age verification guidelines face criticism for restricting access without addressing the root causes of online harm [106, 107].
- Digital-by-default public services and AI-enabled workplaces steadily raise the minimum skill level needed to participate in the economy and society, increasing the risk of exclusion for those who cannot keep up [104].

Impact on European Digital Sovereignty

A digitally low-skilled population is more vulnerable to disinformation, technological lock-in, and dependence on foreign providers, directly constraining Europe's strategic autonomy. When citizens lack the ability to verify information, manage data, or use AI responsibly, power shifts to external platforms and vendors. Low literacy levels reduce public skepticism toward non-sovereign solutions, thereby undermining Europe's capacity to protect its infrastructure and values. By contrast, raising baseline skills enables informed choices, strengthens democratic resilience, and ensures that investments in data governance, cybersecurity, and AI can translate into genuine digital sovereignty.





BUILDING EUROPEAN BIG TECH ALTERNATIVES

Pushing European Solutions Amid US Dominance

Europe's digital sovereignty is at a crossroads. Critical infrastructure and innovation are dominated by US and Chinese platforms (e.g., Amazon and Microsoft), leaving European businesses heavily dependent on foreign providers [108]. This reliance limits the EU's ability to enforce its own rules [109]. It exposes it to extraterritorial reach and risks reducing sovereignty to regulatory theater: Europe can pass laws, but cannot enforce them when foreign providers control the infrastructure. At the same time, trust in Big Tech is eroding due to the proximity of tech leaders to the current US president, Donald Trump. Examples include them taking front-row seats at his inauguration ceremony and Microsoft disabling the International Criminal Court's Office 365 account in the Netherlands after Trump imposed sanctions on its prosecutor [110, 111]. Biased algorithms, repeated privacy and antitrust breaches, and lobbying power in Brussels fuel perceptions that profit consistently outweighs democratic values [112]. While regulations like GDPR and the AI Act set global benchmarks, they remain insufficient without European control over the underlying tech stack.

Facts

- Due to the US's dominance in Europe's tech stack (with a market share of more than 80% in European cloud and 40 out of 58 major AI models in 2024), three in four European businesses would not survive without US tech [73, 113, 114].
- Public trust in Big Tech is declining, yet usage continues to rise, deepening individual dependence [115].
- Nearly half of citizens call for stricter EU tech regulation, while US Big Tech has boosted EU lobbying from 96M EUR (2021) to 113M EUR (2023), now occupying four of the top six lobbying spots [116, 117].

Key Drivers

- Skepticism toward Big Tech is growing, fueled by algorithms that reinforce social biases, such as Meta's job-ad algorithm, which has been shown to exhibit gender bias [118].
- Political tensions over US policies, such as technological "kill switches" (i.e., mechanisms to remotely shut down systems), undermine the reliability of digital infrastructure [111, 119].
- Diverging transatlantic approaches to AI governance create first-mover advantages for European companies that can scale privacy-by-design and explainable AI technologies to global markets [120].

Challenges

- The AI race favors compute-rich ecosystems outside Europe, with US and Chinese firms dominating cloud, GPU infrastructure, and AI-optimized platforms, creating economies of scale and high entry barriers [113, 114].
- European firms struggle to access the large-scale datasets required for competitive AI while complying with privacy and copyright laws [121].
- Fines for Big Tech misconduct, including 700M EUR against Apple and Meta in 2025 and 3B EUR against Google in 2025, have had a limited impact on behavior and failed to deter violations [122, 123, 124, 125].

Impact on European Digital Sovereignty

As US Big Tech firms cultivate ties to the Trump administration, fears of potential "kill switches" in American technology resurface. This fuels growing mistrust in US platforms, even as Europe remains deeply dependent on them for critical infrastructure. Without homegrown AI and cloud ecosystems, European sovereignty risks becoming performative. Genuine digital autonomy requires more than regulating foreign providers. It demands building infrastructure on European soil that embodies European values. By investing in trusted alternatives, Europe can safeguard its cultural identity, bolster its resilience, and shift from being a consumer and "referee" to a technology provider. Only then will businesses and citizens have a genuine choice between US and Chinese Big Tech and competitive European solutions.

RECONCILING EUROPE'S PARADOX OF IDENTITY

Navigating a European Collective Identity Despite Rising Nationalistic Votes

Europe faces a striking duality in public opinion: while nationalism gains support, European identity is also rising. On the one hand, parts of Europe's population struggle with immigration and economic insecurity [126]. These anxieties fuel support for populist and Eurosceptic movements, embedding nationalism and anti-elitism within certain societal groups [127]. On the other hand, public support for EU membership has reached record highs, with more Europeans identifying as such [79, 80]. External crises like the war in Ukraine have strengthened this collective identity, with many viewing the EU as essential for security [81]. Hybrid positions are gaining ground where people combine national pride with support for deeper EU cooperation [128]. This pattern is visible in Finland, Italy, Sweden, and Hungary, where nationalist parties gain votes while overall support for the EU rises [129]. Italy shows this clearest: 88% back stronger EU cohesion yet elected a nationalist government whose current leader pairs nationalist rhetoric with pragmatic EU collaboration [80, 130].

Facts

- In 2022, 32% of Europeans voted for populist, anti-establishment parties on the far left and far right, up from 12% in the early 1990s [82].
- By 2024, seven EU member states had included far-right nationalist parties in their governments [129].
- In 2025, 74% of citizens said EU membership benefits their country, and 89% supported greater unity in addressing global challenges [80, 131].
- Trust in the EU hit an 18-year peak at 52% in 2025, with 75% identifying as EU citizens – the highest share in more than two decades [79, 80].

Key Drivers

- Public anxieties about immigration, perceived cultural loss, and economic insecurity have increased support for populist parties, which capitalize on these fears [132].
- Populist parties exploit social media effectively. For example, Germany's AfD uses TikTok to engage with disaffected young voters, surpassing traditional parties in online reach [133].
- External shocks, including COVID-19 and the war in Ukraine, have strengthened Europeans' sense of unity [81].
- European integration measures, such as Erasmus, open borders, and the euro, have deepened EU identity among younger generations by shaping their daily lives and cross-border experiences [134, 135].

Challenges

- Far-right and nationalist groups are gaining popularity and consolidating around anti-EU rhetoric, which may hinder the coordination of EU policies and actions [136].
- Unequal access to European opportunities, such as education, travel, and study-abroad programs, creates disparities in identification with the EU. Feeling excluded, some groups become more vulnerable to exploitation by populist parties [137].
- National identity remains dominant across Europe, with around 90% of people feeling very close to their nation compared with 40–70% expressing strong European identity [81].

Impact on European Digital Sovereignty

A strong EU identity and trust in EU institutions strengthen digital sovereignty, as citizens identifying as European are more likely to purchase EU-originated products. They also show greater willingness to pay a premium for European products over lower-priced foreign alternatives. However, nationalism at both societal and political levels can hinder these efforts, as Eurosceptic parties may advocate for anti-EU policies. The Italian case illustrates Europe's identity paradox evolving into a hybrid political stance, in which citizens combine national pride with strong EU identification. Leaders use nationalist rhetoric domestically while advancing projects at the EU level. This hybrid approach is likely to spread, shaping sovereignty not as a choice between nation and Europe, but as their synthesis.

LEGAL TRENDS

INFLUENCING THE FUTURE OF DIGITAL SOVEREIGNTY

Pooling European Governance
Steering Data Processing
Boosting EU Digital Policy Efforts
Creating Digital Currency Systems
Reconciling Dual-Use Governance

Palace of Justice in Brussels, Belgium

Adil Köken 
Adrian Stoica 
Ammar Idriz 
Jonathan Mäusle 
Tarak Amouri 

LEGAL TRENDS

Influencing the Future of Digital Sovereignty

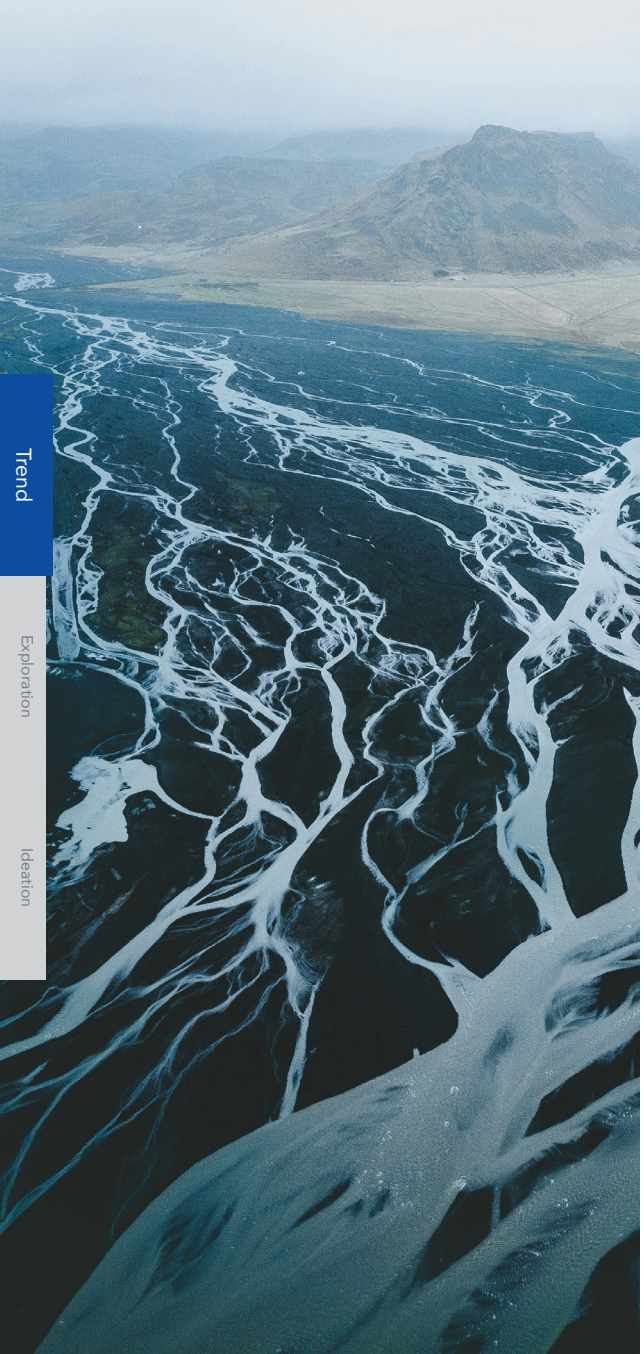
Europe's digital economy has long thrived on openness and global interdependence. It has relied on US cloud platforms to host its corporate data [22], Taiwanese factories to produce its advanced semiconductors [138], and US payment networks to facilitate its online commerce [139]. Yet recent geopolitical conflicts, supply chain disruptions, and the weaponization of technology have exposed deep vulnerabilities [140]. This has shifted the perception of reliance on foreign suppliers from an economic concern to a matter of strategic security. External laws, such as the US CLOUD Act, can still reach into data stored inside Europe, demonstrating that mere geographic residency does not guarantee control [141].

These risks are amplified by Europe's historical fragmentation. With 27 national rulebooks and uneven enforcement, the continent struggles to respond quickly to cyber incidents, coordinate semiconductor supply, or enforce citizen data protection against foreign jurisdictions [142, 143, 144]. The result is a patchwork of regulations and initiatives that leaves Europe slow to react to cross-border crises and poorly positioned to build global tech champions.

In response, the EU is reorienting law and regulation from defensive safeguards into instruments of strategic power, using access to its vast single market as leverage to globalize European standards. Instead of letting foreign providers and frameworks dictate terms, Europe seeks to define its own digital future. Initiatives like the European Digital Decade set measurable 2030 targets [145], while regulatory frameworks such as the GDPR, DMA, DSA, and the Data Act establish a single rulebook for the single market. These measures aim to protect citizens, secure infrastructure, and enhance Europe's ability to influence global technology governance.

This pursuit of digital sovereignty is taking shape through five concrete legal and governance shifts: pooling crisis response and governance across Member States [143, 146], steering data flows to protect information from foreign jurisdictions [147, 148], accelerating policy efforts to close the gap with the US and China [149], building sovereign digital currencies and payment systems [150, 151], and reconciling civilian and military regulation to unlock dual-use innovation [152]. Together, these shifts mark a legal strategy designed not just to regulate markets, but to build Europe's resilience and influence in the digital age.

Europe's ability to translate regulation into operational strength will determine whether it can cultivate a competitive, trustworthy digital market. Success would allow the EU to protect its citizens and values while shaping global norms and standards. The EU can set the foundation to catch up in key technologies like AI while building on its current head start in other areas like post-quantum cybersecurity. Failure, by contrast, risks keeping Europe dependent on external providers and reactive in a world where technological control is increasingly synonymous with strategic power.



POOLING EUROPEAN GOVERNANCE

Advancing Europe's Shift Toward Centralized and One-Rulebook Digital Governance

Europe faces pressing digital risks, including cyber incidents, semiconductor shortages, and cross-border sabotage. Reacting to these threats requires the alignment of 27 individual member state responses and is no longer tenable. To address these risks, the EU is shifting toward pooled governance and unified action, enabling rapid, coordinated responses rather than isolated national efforts. As part of this shift, the EU established central coordination bodies, including the European Cybersecurity Competence Centre (ECCC), the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe), and the European Semiconductor Board, to strengthen research coordination, manage large-scale incident response, and align industrial strategy across member states. Additionally, a single rulebook was introduced to replace differing national laws. These efforts aim to turn political agreements into cross-border action, but their success depends on the quick and uniform enforcement by Member States. Collectively, these steps move Europe closer to a future of reduced fragmentation and greater coherence in digital policy across the single market [143, 146, 153].

Facts

- By February 2025, the EU had imposed 2,394 GDPR fines, up 302 from the previous year, with an average fine of 2.36M EUR since 2018 [154].
- In 2023, 66% of EU firms viewed regulation as an obstacle to investment, compared to 21% in the US, underscoring the potential for uniform rules and enforcement [142].
- The EU-INC proposes an EU-wide company framework. This legal form would sit alongside existing national systems and provide one standardized option for businesses operating across borders, unifying rules for stock options and company structures [155, 156].

Key Drivers

- Recent geopolitical shocks, such as pipeline sabotage and chip shortages, exposed Europe's vulnerability and dependence on external suppliers. This increased the need for shared monitoring and joint crisis-response capacity [157, 158].
- Centralized monitoring and shared threat intelligence create economies of scale. This EU-wide strategy is designed so that each member state strengthens the collective detection coverage and cyber resilience [159].
- Companies are calling for unified regulations across the European Single Market to minimize the need for multiple compliance adjustments when entering different national markets [160].

Challenges

- Unequal national enforcement of rules and laws lets companies exploit regulatory gaps. In response, the European Data Protection Board (EDPB) is launching new guidelines and procedures to align enforcement across the Union [161].
- Disagreements over how much control should remain with individual countries slow EU decision-making. For instance, the NIS2 directive, designed to elevate cybersecurity standards across the EU, had not been fully adopted by nearly half of the member states in mid-2025, delaying its uniform adoption [144].
- A single rulebook may oversimplify specialized industries, while optional frameworks risk low uptake and limited impact [162].

Impact on European Digital Sovereignty

Pooling governance is about more than streamlining regulations: it fundamentally reshapes Europe's position within the global digital landscape. More consistent law enforcement reduces uncertainty for firms and could make the EU a more attractive hub for scaling high-tech businesses. Additionally, through coordinated crisis response, Europe can significantly enhance its infrastructure resilience. At the geopolitical level, stronger coordination would strengthen Europe's influence in international standard-setting, enabling it to reduce dependencies on US and Chinese frameworks. Ultimately, the fundamental lever lies less in individual regulations and more in the EU's ability to translate pooled governance into concrete sovereignty gains [163].

STEERING DATA PROCESSING

Securing Data Flows to Strengthen Europe's Digital Sovereignty

Data steering is the strategic management and control of data flows, storage, and processing. It extends beyond storing data within a jurisdiction and actively directs how and where data is moved to comply with regulatory, privacy, and security requirements. Technically, it involves routing control systems that restrict data to approved locations and secure infrastructure, ensuring both legal and operational control. European frameworks, such as the AI Act or the Digital Operational Resilience Act (DORA), establish compliance standards that define data handling practices and compel organizations to align with sovereignty principles [147, 148]. Data steering is essential for Europe to establish itself as a leader in the digital space, as other regions increasingly look to European legislation for legal guidance [164]. Yet this regulatory ambition is in stark contrast to the persistent dependency: cloud and data infrastructure remain dominated by US and Chinese providers, with Europe struggling to develop competitive solutions [165]. Regulation thus aims to protect European interests on an international stage while incentivizing local innovation. This dual approach aims to shift Europe from dependence to leadership in global data standards [166].

Facts

- Over 80% of Europe's digital services and products are imported, and 92% of data is stored on US-based cloud servers [167].
- The AI Act establishes clear rules for steering data based on risk levels for AI systems. It bans use cases such as social scoring and requires strict checks for "high-risk" systems in areas like hiring and healthcare [168].
- The DORA aims to create room for multiple cloud providers, ensuring that no single vendor becomes too dominant, thereby risking systemic failure [148].
- Responding to European concerns, major US cloud providers like Microsoft and AWS begin to offer sovereign cloud solutions to provide more control and data residency within Europe [169].

Key Drivers

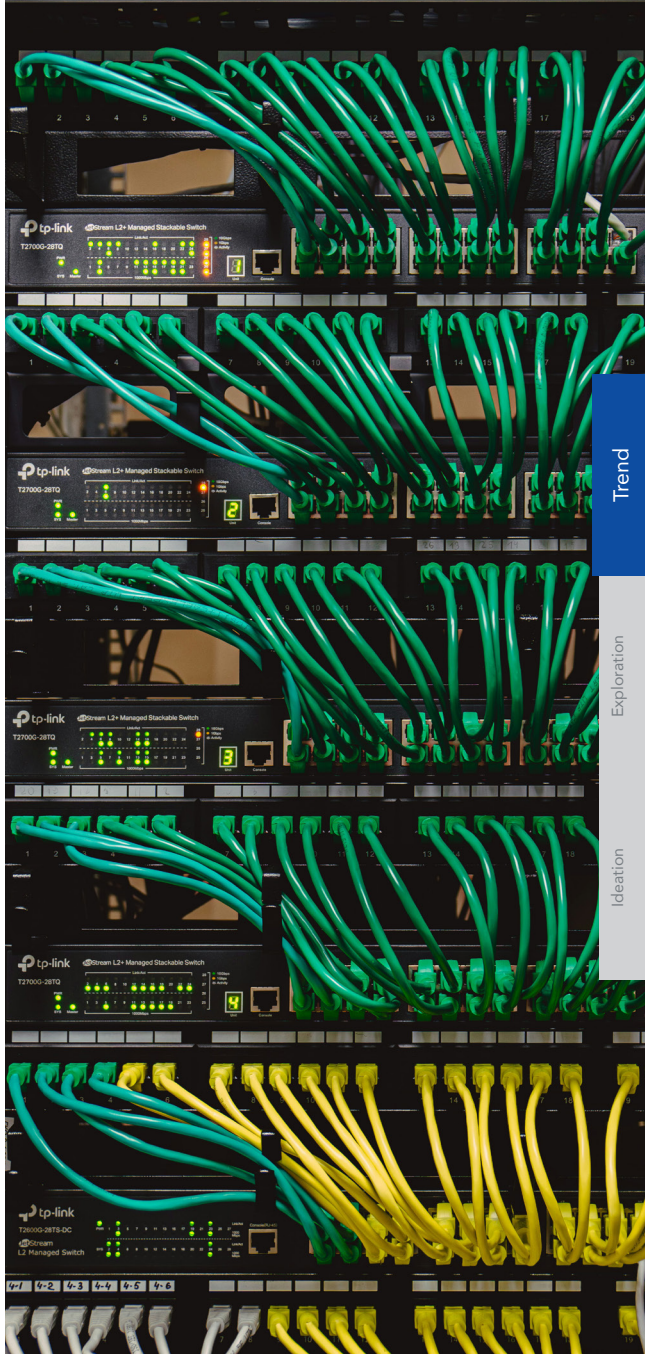
- As data becomes a geopolitical and economic asset, the EU's profound dependency on foreign infrastructure, where 92% of its data resides on US servers, has made data steering a strategic necessity [167, 170].
- Due to jurisdictional overreach, physical data storage in Europe does not guarantee legal protection. Under laws like the US CLOUD Act, US authorities can demand access to data held by US companies, even from servers within the EU, as demonstrated in legal disputes involving major US cloud providers [141]. This nullifies the security promised by mere data residency.
- Fragmented European capabilities slow the development of competitive cloud and data infrastructure, risking initiatives becoming symbolic rather than delivering genuine sovereignty [171, 172].

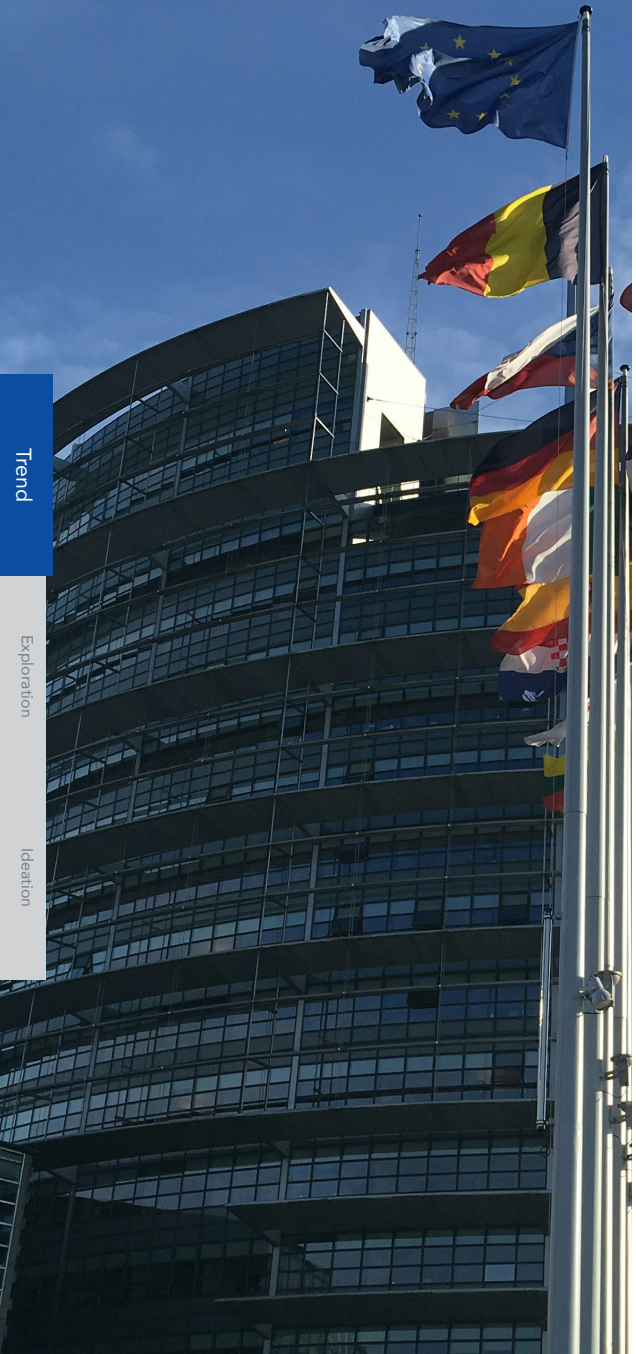
Challenges

- Overcoming the entrenched market dominance, technical advantages, and vendor lock-in of established non-EU cloud providers remains a significant barrier to achieving genuine market sovereignty, even as European alternatives emerge [173].
- Compliance with EU regulations creates administrative and financial burdens, especially for smaller companies. At the same time, unresolved conflicts with foreign laws highlight the need for more precise legal definitions and new instruments to manage jurisdictional clashes [171, 172].

Impact on European Digital Sovereignty

Effective data steering strengthens Europe's digital sovereignty by creating a predictable and secure environment for innovation and investment in AI, cloud, and digital services. By establishing clear operational standards, European firms can compete with greater confidence and attract resources to develop homegrown solutions. With data becoming increasingly important, operational control provides strategic leverage in global negotiations, enabling Europe to influence international rules and standards. This foundation allows the EU to proactively regulate emerging technologies, turning data sovereignty into both a competitive advantage and a long-term enabler of European digital leadership.





BOOSTING EU DIGITAL POLICY EFFORTS

Bridging the Digital Gap with Clear Targets and Coordinated Policy Action

The EU has long trailed behind digital frontrunners like the US and China. To close this gap, it launched the Digital Decade programme in 2022 – a comprehensive strategy with clear targets for 2030. Key areas include boosting digital skills, driving business transformation, building secure infrastructure, and digitizing public services [78]. To ensure this transformation reflects European values, the EU adopted the Declaration on Digital Rights and Principles alongside the programme. While the Digital Decade defines the goals, the Declaration provides the framework to reach in a way that protects privacy, freedom of choice, inclusion, and democracy [149]. This link between action plan and guiding principles materializes in measures such as the Cyber Resilience Act, which mandates cybersecurity standards for all digital products in the EU. It strengthens critical infrastructure, protects users from growing threats, and builds trust through transparency [174]. Together, these initiatives mark Europe's effort to shape a value-driven digital future.

Facts

- National Digital Decade roadmaps outline 288.6B EUR in planned investments and structural reforms aimed at creating sustainable, secure, and human-centered digital ecosystems across Europe [78].
- According to the 2024 State of the Digital Decade report, 45% of EU-level recommendations have already shown significant progress, particularly in areas such as human-centered AI and the protection of fundamental digital rights [78].
- The Declaration on Digital Rights and Principles establishes a guiding framework that places people and their rights at the very core of Europe's digital future [149].

Key Drivers

- Public support drives embedding values into the digital sphere, with 85% of EU citizens supporting government initiatives to tackle online misinformation compared to only 55% in the US [175, 176].
- Achieving the Digital Decade 2030 targets could boost the EU's GDP by up to 1.8%, underscoring the strong link between digital advancement, sustainable economic growth, and global competitiveness [78].
- The intensifying competition from the US and China drives the EU to accelerate its digital policy agenda to stay resilient, maintain global relevance and decision-making power in the digital economy era [149].

Challenges

- Although the targets demonstrate strong ambition, actual implementation often lags. Nearly half of the EU-level recommendations in the 2024 State of the Digital Decade report show only limited or no progress. Basic digital skills among citizens only increased by 2% since 2020, reaching 55% in 2025. This slow progress falls way short of the 80% goal for 2030 [78].
- Regulations such as the Cyber Resilience Act (CRA) face resistance to implementation due to fragmented legal frameworks and industry lobbying [177].

Impact on European Digital Sovereignty

The EU's Digital Decade 2030 programme and Declaration on Digital Rights lay the foundation for a human-centered digital future in Europe. Public backing for tackling disinformation and online threats gives strong societal momentum. However, slow progress in adopting even basic digital skills and opposition to regulation such as the CRA risk Europe falling short of its ambitious transformation targets. Overcoming these challenges would prove that citizen privacy, democratic systems and economic interests can be protected simultaneously. In contrast to the US or China, the EU could establish itself as the leading digital role model and ultimately secure European interests on a global scale.

CREATING DIGITAL CURRENCY SYSTEMS

Building a Digital Euro and Payment Systems to Secure Europe's Monetary Independence

The EU is building a sovereign digital currency and payment systems to protect monetary autonomy in the digital age [178]. Today, most Eurozone card payments are processed by international, primarily US-based providers, creating strategic dependencies [179]. To address this risk, the EU is establishing new regulatory frameworks and digital infrastructure to reinforce control over payments. Central to this effort is the digital euro: a free, secure, and universally accessible form of digital cash issued by the European Central Bank (ECB) [179]. The EU also expands fast payment options like SEPA Instant and backs the European Payments Initiative (EPI) and its "Wero" wallet [180]. This is complemented by creating regulatory certainty for emerging products such as crypto-assets and other fintech innovations [181]. Collectively, these initiatives aim to protect consumers, reduce foreign reliance, and foster a resilient, competitive European payments ecosystem [151].

Facts

- The European Commission has proposed to establish the digital euro as a legal tender. Once enacted, most merchants in the Eurozone would be required to accept it [151].
- The Open Finance Framework, Payment Services Directive 3 (PSD3), and Markets in Crypto-Assets Regulation (MiCA) create a harmonized rulebook that mandates data sharing, unifies licensing, and provides regulatory certainty [150, 181].
- The EPI, backed by 16 major European banks and providers, launched the "Wero" wallet as a European-governed, instant account-to-account payment solution, designed to reduce reliance on international card schemes [182].

Key Drivers

- More than 60% of EU card payments are still processed through non-European networks, exposing Europe to external control and potential service disruptions. This necessitates the development of local solutions strengthening Europe's payment infrastructure [139].
- The rapid growth of stablecoins, big-tech wallets, and foreign cryptocurrency exchanges threaten the euro's leading role in the European monetary system. This weakens monetary policy effectiveness, making it imperative for Europe to accelerate sovereign digital finance solutions [183].
- Operational and especially cyber resilience become increasingly important due to the evolving threat landscape. Secure, EU-governed payment rails are crucial to ensure continuity of critical financial services even in crises [179, 182].

Challenges

- Due to fragmentation and bureaucratic barriers, the digital euro rollout remains slow and uncertain, enabling foreign digital currencies to take dominant market positions [184].
- The design of open and flexible standards requires balancing inclusivity, interoperability, and practicality to ensure interoperability without creating barriers that favor large, incumbent providers or exclude smaller players, promoting a level playing field [185].
- Enabling cross-currency instant payments introduces complexity. The coordination across regulatory regimes, multinational providers and exchange-rate management requires careful design [186].

Impact on European Digital Sovereignty

The EU strives to reduce reliance on foreign providers and secure monetary independence by rolling out the digital euro and sovereign payment systems. A unified European financial ecosystem promises to accelerate payments, strengthen consumer protection, and expand fintech opportunities. However, challenges such as aligning diverse member states and balancing innovation with regulation persist. Overcoming these barriers is crucial for maintaining control over Europe's financial infrastructure and monetary policy. With effective implementation, Europe can foster its sovereignty in the financial domain.

RECONCILING DUAL-USE GOVERNANCE

Unifying Regulatory Frameworks to Enable Dual-Use Innovation

Europe's innovation in dual-use technologies is increasingly constrained by regulatory misalignment. EU policymakers maintain strict boundaries between civilian and military domains, yet the technologies themselves no longer adhere to these divisions [152]. This artificial separation generates regulatory inefficiencies and ultimately fragments innovation ecosystems, creating redundancies, and increased compliance costs [187]. Dual-use technologies have become increasingly common across sectors: The Global Positioning System (GPS) serves both private vehicles but also military drones. The underlying functionality does not change with the application, yet EU regulations impose differentiated treatment. By contrast, the US and China leverage technological convergence as a strategic asset, actively incentivizing cross-sector development to accelerate innovation and strengthen competitiveness [188].

Facts

- The EU sources over 60% of its drone components from the US and China, leaving Europe vulnerable to geopolitical pressure or export restrictions [187].
- The AI Act and Horizon Europe both enforce a strict separation between civilian and military domains: the former excludes military applications altogether, while the latter explicitly prohibits military involvement [187, 189].
- The "Readiness 2030" whitepaper, published by the European Commission in 2025, announced that the European Innovation Council (EIC) plans to invest in dual-use technologies, lifting the previous civilian-only mandate [152].

Key Drivers

- Russia's invasion of Ukraine and the US questioning NATO commitments forces the EU to reconcile defense autonomy with dual-use realities. With 64% of arms being imported from the US, Europe faces an urgent need to develop sovereign capabilities through the very dual-use technologies it has historically restricted [190, 191].
- Technological convergence between civilian and military applications drives pressure to unify regulation. Advanced civilian and military drones are powered by the same AI systems, sensors, and components [192, 193].

Challenges

- The EU lacks a standard definition of "dual-use." For instance, the European Investment Bank (EIB) and export control authorities apply different definitions, hindering decision-making for joint investments [187].
- EU regulations struggle to keep up with rapidly evolving technologies. By the time dual-use frameworks are adopted and implemented, the underlying technologies have already advanced [194].
- The EU lacks a central licensing system, while member states establish a patchwork of national dual-use controls [194]. The same technology permitted for export in one country may be banned in another, creating regulatory fragmentation.

Impact on European Digital Sovereignty

Regulatory fragmentation poses a serious risk to the EU's defense capabilities and digital autonomy. It prevents companies from achieving the necessary scale to compete globally, as they cannot seamlessly leverage civilian innovations for defense applications like their US and Chinese counterparts. The disconnect between ethical positions and investment strategies creates policy uncertainty that deters long-term R&D investments in autonomous systems. A path forward would be a unified framework that bridges the civilian and military domains. This could accelerate technological development in the EU and reduce European dependence on foreign technologies for both defense and commercial needs.

ECONOMIC TRENDS

INFLUENCING THE FUTURE OF DIGITAL SOVEREIGNTY

Balancing Growth and Dependency
Modularizing Digital Supply Chains
Driving Strategic Collaboration
Turning Defense into a Digital Advantage
Closing the Funding Gap

Royal Exchange in London, England

Amelie Pöhnitzsch 
Edwin Daniel 
Jakob Limmer 
Karolina Wick 
Niklas Remiger 

ECONOMIC TRENDS

Influencing the Future of Digital Sovereignty

The debate on digital sovereignty is often framed in political or technological terms. Yet its foundations are ultimately economic as well. Digital technologies have become an integral part of the modern economy. Their centrality is reflected most visibly in the stock markets, where the world's most valuable companies are no longer traditional manufacturers or energy giants, but digital platforms and infrastructure providers. NVIDIA's market capitalization alone surpassed 4.32T USD on September 6, 2025 [195], nearly double the combined capitalization of all companies listed in Germany's DAX index, which stood at above 2.39T USD on the same date [196]. Europe faces an economic challenge to restructure its digital foundations as technological dependencies increasingly threaten its economic competitiveness and growth prospects. Control over digital infrastructure, platforms, and data translates directly into control over markets and value creation [108]. The past decade has brought major shocks: a pandemic, broken supply chains, war in Europe, and growing geopolitical tensions. Together, they prove that economic resilience is far from guaranteed [197].

Over 80% of Europe's digital technologies are currently imported. European companies account for just 7% of global software and internet research spending, making the urgency for change clearer than ever [1]. The concept of digital sovereignty is evolving into an EU strategic priority, aiming to strengthen control over critical digital infrastructure and reduce reliance on non-European stakeholders [108]. This shift presents an opportunity to reimagine Europe's position in the global economy while preserving its values and competitive advantages.

Five key economic trends play into this opportunity to make Europe's economy more sovereign. One of these is the modularization of production, which is revolutionizing supply chains. It creates sovereign components that reduce systemic risks and enable rapid adaptation to disruptions [198]. Strategic collaborations are pooling resources and expertise across public-private partnerships to promote European companies. These collaborations accelerate the development of sovereign infrastructure, such as Gaia-X [199]. Defense-driven innovation is catalyzing technological advancement. Increased military spending can create spillover effects in dual-use technologies, particularly in the areas of AI and cybersecurity [200]. The digital economy's expansion continues to reshape all sectors. It exposes concentration risks that necessitate European alternatives to global tech giants [1]. Finally, regulatory incentives and large-scale sovereign technology investments address the chronic shortage of growth capital. This shortage has historically forced European startups to relocate abroad [201].

These interconnected trends are pointing the way forward for a sovereign European economy. Digital sovereignty emerges as Europe's strategic response to economic vulnerabilities exposed by global disruptions. Businesses, governments, and the European Commission are challenged to build this future together.

BALANCING GROWTH AND DEPENDENCY

Navigating the Double Edge in the Digital Economy

The digital economy encompasses all activities that rely on digital information, use modern information networks, and depend on ICT for efficiency and growth [202]. It has expanded rapidly, transforming society and individuals' daily lives. From finance, retail to manufacturing, agriculture, and healthcare, digital innovations are reshaping business models and services worldwide [203]. The digital economy is projected to reach 17% of global GDP by 2028 [204]. Billions of people and devices are coming online, fueling new digital services and markets [205, 206]. Yet this expansion also creates dependencies, as economic value and critical infrastructure concentrate in a few global technology companies. This concentration amplifies economic risks, making resilience and sovereignty central concerns for decision makers [1]. Multinational projects aim to reduce EU vulnerabilities and dependencies in digital supply chains, strengthening resilience [207]. The rise of the digital economy comes at a cost: it reshapes people's daily lives while increasing Europe's reliance on external technology providers.

Facts

- The ICT sector is growing faster than the overall economy and is projected to reach 16.5T USD globally by 2028, which highlights its increasing influence on global economic performance [208].
- The AI market is expected to grow 27% per year, reaching a volume of 1.01T USD by 2031 [209, 210].
- TSMC dominates more than 50% of the global semiconductor market and 90% of advanced chip production [1]. While Amazon, Microsoft, and Google account for 70% of the European cloud infrastructure market [211]. This shows the digital economy's reliance on a few non-EU players.

Key Drivers

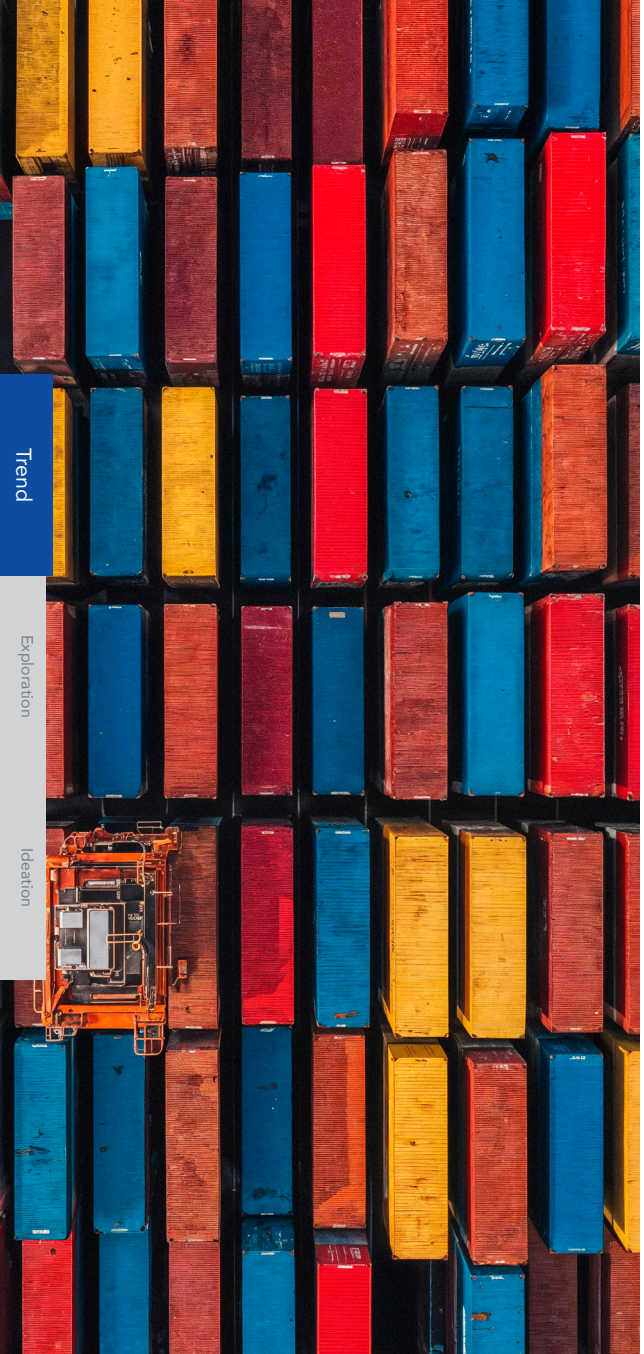
- Declining costs of computing, storage, and bandwidth are driving the widespread adoption of digital platforms, large-scale operations, and data-driven services [212].
- The rapid increase in Internet access and mobile technology is creating a global consumer base for digital services. Over 5.5B people, nearly 68% of the world's population, are Internet users [205].
- Rising awareness of economic risks from dependencies on non-EU technology providers is driving supportive policies and public investments aimed at strengthening local capacity [207].

Challenges

- The intangible nature of digital services complicates the determination of tax bases and the allocation of profits, making it difficult for European countries to effectively tax these services [213].
- Fragmented digital infrastructure across EU countries limits interoperability and scalability, slowing innovation and reducing the continent's ability to compete globally [1].
- Europe's underinvestment in cutting-edge technologies and limited translation of R&D into commercially successful innovations slows growth in digital sectors and reduces competitiveness compared to global leaders [1].

Impact on European Digital Sovereignty

The growth of the digital economy in the EU has created both opportunities and vulnerabilities for digital sovereignty. Innovations such as AI are vital drivers of economic growth and competitiveness, enabling efficiency gains across sectors. On the other hand, the EU's digital economy remains heavily reliant on non-EU technology companies, with most data stored on US-owned servers. This creates economic vulnerabilities by limiting Europe's ability to capture the full value of digitalization and exposing critical infrastructure to external control. Without more substantial investment, integration, and support for EU-based firms, this imbalance poses a threat to long-term economic growth and strategic autonomy [214].



MODULARIZING DIGITAL SUPPLY CHAINS

Reducing Single Dependencies to Boost European Competitiveness

Digital supply chains are sharply affected by global shocks such as COVID-19, trade disputes, and energy crises, particularly in sectors like semiconductors, cloud infrastructure, and digital hardware [215]. Since digitalization underpins industrial and service value chains, Europe's dependence on non-European stakeholders increases risks beyond the IT sector [216]. Traditional resilience strategies such as reshoring, nearshoring, and partner-shoring aim to reduce exposure to shocks but still involve costly relocation [217]. A more dynamic layer is emerging through modularization, which restructures supply chains into interoperable components and reduces systemic risk by limiting interdependencies [198]. If a module is disrupted, alternatives can be integrated seamlessly to sustain operations and innovation. Combining modular supply chain design with targeted policies, Europe can boost resilience while promoting competitiveness and technological sovereignty. EU initiatives like the Chips Act, Critical Raw Materials Act, and Digital Markets Act support this shift by securing semiconductor production and ensuring fair competition in the digital economy. [218].

Facts

- Recent data show that 37% of EU companies face major difficulties obtaining raw materials and semiconductors, while 34% report significant disruptions in logistics and transportation [219].
- Modularizing industrial supply chains can boost EBIT by 3–9% through streamlined value chains and shorter production lead times, with lower material costs adding 2–6%, reduced manufacturing costs 1–2%, and decreased order engineering and investment costs 0–1% [220].
- Globally, only 6% of companies achieved end-to-end visibility of their supply chains with disruptions costing companies about 8% of their annual revenues [221, 222].

Key Drivers

- Recent crises such as the COVID-19 pandemic, strategic raw material shortages, and rising shipping costs have revealed vulnerabilities and single points of failure in global supply chains, prompting Europe to diversify suppliers and strengthen domestic resilience to protect competitiveness and stability [219].
- Rising geopolitical tension, including threats to digital trade, cyberattacks, and export bans, have accelerated European efforts to reclaim sovereignty over critical technologies and platforms [223].

Challenges

- Europe's push to modularize digital supply chains is hindered by the semiconductor industry's global fragmentation, with production, design, raw materials, and assembly dispersed across regions. Despite niche strengths in equipment and automotive chips, Europe remains relatively underrepresented [224].
- Persistent reliance on non-European providers for critical technologies limits interoperability in the European digital ecosystem and hinders homegrown innovation [225].
- The cyber attack surface expands, increasing potential entry points for adversaries and requiring greater coordination on cybersecurity standards [226].

Impact on European Digital Sovereignty

Critical technologies such as semiconductors and cloud infrastructure depend on stable access to raw materials and advanced manufacturing [218]. Disruptions or foreign dependencies in these areas directly undermine Europe's ability to innovate and control its digital future. By embedding resilience in core digital product supply chains through modularization, the EU can reduce the risk of sudden tech cut-offs, strengthen regional tech standards and innovation, and protect strategic sectors from external price shocks and supply disruptions [219]. This enables Europe's economy to shape its digital future, set technological norms, and maintain economic resilience in a volatile global environment.

DRIVING STRATEGIC COLLABORATION

Leveraging Public-Private and Private-Private Partnerships for Digital Growth

Europe's competitiveness is increasingly shaped by collaborative ecosystems that go beyond traditional regulation and subsidies. Public-private partnerships and private-private alliances are emerging as critical mechanisms to co-develop, deploy, and scale digital infrastructure and services [227]. Flagship initiatives like Gaia-X demonstrate how federated, interoperable cloud and data frameworks can be created through collective action [228]. The cooperation of leading automotive players on shared software platforms illustrates how even fierce competitors must collaborate to meet rising technological complexity [229]. These developments are increasingly fueled by academia-industry consortia, which align research capacity with market needs and strengthen innovation ecosystems [230]. By combining complementary strengths, these partnerships unlock efficiencies, reduce costs, and accelerate Europe's ability to compete globally [227]. Together, they mark a shift from isolated efforts toward coordinated ecosystems that pool resources, accelerate innovation, and enhance Europe's competitive position.

Facts

- Founded in 2020, Gaia-X has grown into a network of over 250 organizations from across 30 countries, including both leading companies and public institutions [231].
- The EU's InvestAI initiative will allocate 200B EUR to fund five AI gigafactories via public-private partnerships, with governments covering up to 35% of the investment and industry contributing the remainder [232].
- In June 2024, eleven major automotive players, including BMW, Mercedes-Benz, Volkswagen, Bosch, and Continental, agreed to jointly develop S-CORE, a shared open-source middleware platform for vehicle software [229].

Key Drivers

- With an R&D investment gap of 750–800B EUR each year, Europe relies on public-private collaboration to bridge financing and strengthen innovation capacity [233].
- EU programs such as Horizon Europe, Digital Europe, and IPCEI incentivize collaborative R&D and deployment models by enabling cross-border and cross-sector investment [234].
- Academia-industry consortia like the TUM Think Tank foster collaboration by aligning policy, technology, and practice, providing stakeholders with frameworks, pilots, and shared knowledge to advance cloud and digital sovereignty [230].

Challenges

- Companies often hesitate to share data, IP, or infrastructure over fears of competitive disadvantage [235].
- Conflicting incentives complicate collaboration, with governments prioritizing sovereignty, ethics, and accountability and firms focusing on competitiveness, profitability, and scalability [236].
- Accessing EU or national funding often requires navigating complex application, compliance, and auditing procedures, which can deter SMEs (small and medium enterprises) or startups from participating fully in collaborative projects [234].

Impact on European Digital Sovereignty

Collaborations across public and private sectors are laying the foundation for Europe's digital sovereignty. By fostering co-owned and interoperable infrastructures, they reduce dependence on non-European platforms while ensuring that innovation aligns with EU values and standards [228]. These partnerships transform digital sovereignty from a political aspiration into an economic reality, embedding trust, scale, and competitiveness into Europe's digital ecosystems. However, their long-term success depends on addressing structural barriers, including limited trust and data-sharing, divergent priorities between stakeholders, and accessibility gaps that hinder the broad participation of smaller players [234, 235, 236].

TURNING DEFENSE INTO A DIGITAL ADVANTAGE

Defense as a Catalyst for Technological and Digital Sovereignty in Europe

After underinvesting in defense for many years, the EU as a collective and its individual member states are drastically increasing defense spending due to intensified geopolitical tensions. A temporary 1% of GDP increase in military spending could boost Europe's long-term GDP by 0.25% per year through innovation spillover. Key technologies such as GPS or the Internet are examples of spillovers initially developed by the military [200]. This surge in investment combined with growing demand for digital warfare technologies offers opportunities to build new ecosystems and startups vital for technological independence from actors outside Europe [237]. Quantum Systems and Helsing, German startups working on autonomous aircrafts, drones and software-enabled warfare reached enterprise values of 1.1B EUR and 13.2B EUR respectively [238, 239]. These valuations illustrate the rapid growth and market potential of European defense tech startups. Further innovation beyond defense, especially in dual-use sectors such as AI and cybersecurity, is expected to follow from the increased defense efforts in Europe [240].

Facts

- EU defense expenditure increased by 19% from 2023 to 2024, reaching 343B EUR [241]. This upward trend is expected to continue as NATO members committed to invest 5% of GDP into defense by 2035 [242].
- The European Commission's ReArm Europe 2030 plans to mobilize over 800B EUR in defense, including a 150B EUR loan instrument for procurement [243].
- Investments into European defense tech startups increased by over 500% in the 2021 to 2024 period compared to the preceding three years [237].

Key Drivers

- Warfare is increasingly evolving toward hybrid forms, including cyber operations and autonomous systems, with the Ukraine-Russia conflict highlighting the growing significance of uncrewed platforms. NATO has acknowledged the urgent need to rapidly enhance its capabilities in autonomous systems [244].
- Europe's reliance in the 2000s and 2010s was spread across Russia, the US, and China for energy, security, and trade, but this dependence has gradually shifted toward the US [245].
- Military assets such as the F-35 fighter jet are turning into software-reliant goods that require continuous and regular software updates [246].

Challenges

- Europe is heavily dependent on the US for key systems, with US-based arms imports reaching 64% in 2024 [247]. Without a concentrated effort to build these capabilities, a majority of investments will flow to the US and cause further dependencies.
- In Europe, military procurement follows lengthy, drawn-out cycles, which often clash with the rapid development typical of venture-backed innovations [248].
- Military procurement heavily favors national production. Therefore, Europe operates over 170 weapons systems versus 30 in the US, and lacks large, multinational defense companies [249].

Impact on European Digital Sovereignty

Increasingly, military sovereignty is defined by technological sovereignty. The demand for European-built combat technologies is rising. This surge could catalyze digital sovereignty by boosting innovation in AI, cybersecurity, and autonomous solutions. Challenges include bureaucratic, fragmented procurement and a reliance on US arms [248, 250]. Unless public and private actors coordinate their efforts, substantial defense investments may have little effect on Europe's economy and digital sovereignty. Effectively leveraging these investments could strengthen Europe's digital capabilities, reduce dependence on external actors, and enhance strategic autonomy.

CLOSING THE FUNDING GAP

Enforcing Capital and Regulatory Incentives for European Startups

Closing the late-stage funding gap highlights Europe's growing effort to address its underinvestment in scaling digital startups. As of January 2025, the EU has 110 unicorns and the UK 55, while the US counts 687, showing Europe's weaker performance [251]. Despite a strong pipeline of early-stage ventures, European firms face challenges in securing growth capital, particularly in strategic sectors like cloud, AI, semiconductors, cybersecurity, and advanced computing [252]. It also reflects how fragmented markets and regulatory inconsistencies make coordination harder, limiting strategic alignment and discouraging large-scale investment [253]. Because late-stage growth funding remains scarce, many firms cannot scale. Instead, they move abroad, often to the US, to tap stronger venture capital and public markets [254]. US venture funds and capital markets consistently provide larger late-stage rounds, enabling faster scaling and global reach. On the contrary, European founders often sell early or seek US IPOs, leading to a loss of intellectual property, talent, and economic value [251].

Facts

- Europe invests significantly less in late-stage tech ventures compared to the US and China, with EU-based startups receiving only around one third of the growth capital available to their US counterparts [255].
- Between 2008 and 2021, around 30% of Europe's unicorns moved abroad, mainly to the US [254].
- European sovereign wealth funds, such as France's "French Tech Souveraineté" and Germany's "Zukunftsfonds" are actively investing in tech startups to keep strategic assets and IP within the EU. These initiatives represent a growing consensus that digital autonomy cannot be achieved without direct capital intervention [256, 257].

Key Drivers

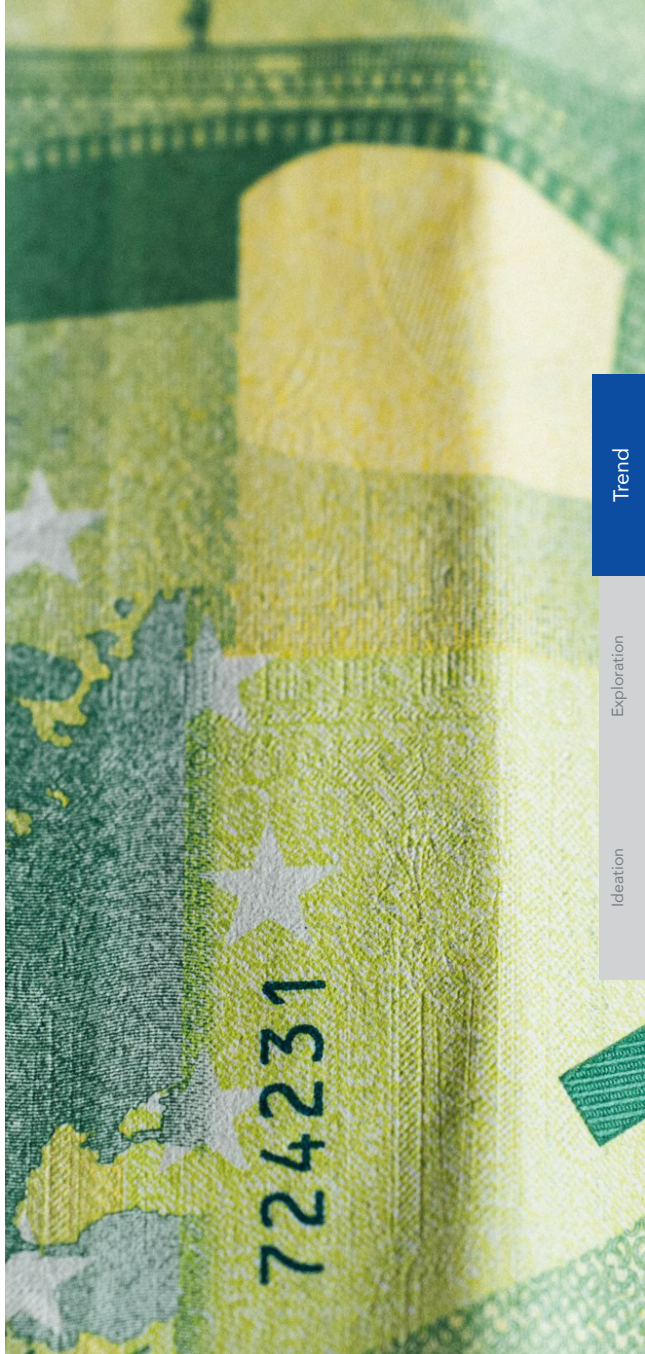
- A fragmented venture ecosystem makes cross-border fundraising complex and costly. This limits liquidity and investor participation in growth-stage financing for European startups [258].
- Many European startups rely on US venture funds for growth capital leading to capital flight and startup brain drain [259].
- The US CHIPS Act, which funds domestic semiconductor production, and other countries' initiatives have prompted the EU to respond with similar sovereignty-oriented investments, such as those stemming from the EU Chips Act [260].

Challenges

- EU-level initiatives often suffer from slow rollout and administrative burdens. Startups need speed and simplicity, but incentive programs and funding can be complex and inaccessible. Many pan-European funding initiatives remain nationally siloed, slowing progress toward integrated digital infrastructure [252].
- A shortage of skilled labor in strategic sectors like semiconductors, AI, and cybersecurity, projected to exceed 75,000 unfilled positions in the EU semiconductor industry by 2030, limits the effective use of funding. Without investment in education and workforce development, funding alone can not close the sovereignty gap [261].

Impact on European Digital Sovereignty

Startups are key to developing Europe's future leaders in AI and other critical technologies, as supported by the European Commission's AI Innovation Package for startups and SMEs [262]. Capital and regulatory incentives enable startups to secure late-stage funding and scale internationally [263]. This reduces reliance on foreign investors and markets while keeping strategic technologies under European ownership and control. Instruments like sovereign tech funds, targeted tax incentives, and integrated capital markets, support technological autonomy, economic resilience, and the EU's ability to set its own digital standards [264].



ENVIRONMENTAL TRENDS

INFLUENCING THE FUTURE OF DIGITAL SOVEREIGNTY

Leveraging Climate Directives
Enabling Circular Tech Lifecycles
Powering Clean Energy
Greening Digital Infrastructure
Reusing Existing Infrastructure

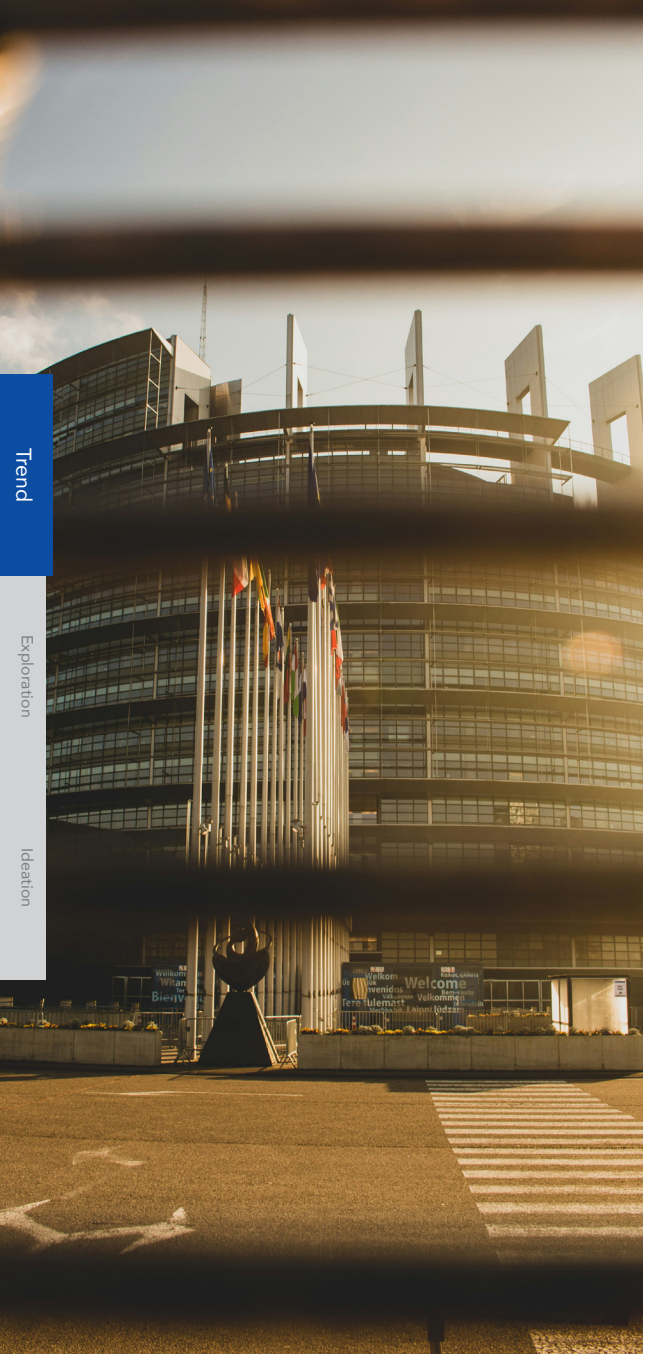
Bosco Verticale in Milan, Italy

Benedikt Albertsen 
Charlotte Schöllkopf 
Jinjun Dong 
Katy Grossmann 
Linnea Brand 

ENVIRONMENTAL TRENDS

Influencing the Future of Digital Sovereignty

Every economic activity, from agriculture to high technology, relies on energy, raw materials, and stable environmental conditions. Climate change acts as a systemic factor that destabilizes supply chains, energy systems, and infrastructure [265]. Since digital infrastructures such as cloud services, AI clusters, and telecom networks rely on these same foundations, environmental resilience is essential for sovereignty. But environmental pressures will intensify in the coming decades. For Europe, risks are further amplified by its structural dependence on external suppliers of energy and critical materials [266]. This reliance exposes the continent to potential restrictions on fossil fuels from Russia and the Middle East, as well as on rare earths and lithium processed in China, which can be used as tools of geopolitical leverage [266, 267]. Ultimately, digital sovereignty must be connected with environmental resilience, as it forms the foundation for Europe's sovereignty. This interaction runs in both directions. Many climate measures strengthen sovereignty by reducing dependency and increasing resilience, for example, through energy efficiency, renewable energy, or circular material use [268, 277]. However, measures can also create conflicts when raising costs, weakening competitiveness, or increasing reliance on imports of key green technologies [269]. Simultaneously, the drive for strategic autonomy supports investments in renewable energy and recycling, which also advance climate goals [270]. The result is a close yet differentiated relationship where many actions create dual legitimacy even though the two agendas are not identical. The tensions between climate measures, costs, and new dependencies unfold across three dimensions: Scale and speed, interdependence of infrastructures, and legitimacy and acceptance. Europe's digital sovereignty is shaped by how it manages environmental constraints across them. Firstly, scale and speed matter because digital demand grows rapidly through AI, cloud computing, and 6G [271]. Unless the energy transition and material cycles expand at the same speed, the external dependencies outlined above only intensify. Clean energy must be deployed faster than demand, recycling scaled beyond pilots, and industrial land reused for data centers before bottlenecks lock in [272]. Secondly, the interdependence of infrastructures is crucial since digital systems rely on natural systems. Droughts reduce cooling water, storms damage grids, and energy crises affect cloud and AI services. This reflects systemic risks where climate shocks destabilize supply chains and energy systems [265]. Environmental stability thus becomes a direct condition of sovereignty. Thirdly, legitimacy and acceptance determine whether sovereignty projects succeed, as they consume land, water, and energy Here, the duality described earlier is visible: measures may strengthen sovereignty long term but trigger costs and resistance short term [273]. Moreover, brownfield reuse has more societal support compared to building infrastructure from scratch, while also lowering the carbon footprint through the reuse of existing facilities [274]. Together, these dimensions sharpen the argument that the environment is the condition of sovereignty. The following five trends on climate directives, circular lifecycles, clean energy, efficiency, and brownfield reuse illustrate how environmental resilience and digital sovereignty converge in practice.



LEVERAGING CLIMATE DIRECTIVES

Pairing Climate Targets With Energy and Supply-Chain Resilience Through Binding Rules

Climate change will increasingly disrupt supply chains and transport routes through extreme weather, posing direct risks to Europe's digital infrastructure [265]. To address these shocks, Europe must not only meet its climate targets but also strengthen its supply chain resilience. At the same time, the rising energy demand from the expansion of data centers and AI clusters increases Europe's strategic vulnerability due to its reliance on energy imports from foreign suppliers [267]. Two directives address these vulnerabilities. The Corporate Sustainability Reporting Directive (CSRD) and the European Sustainability Reporting Standards (ESRS) require firms to disclose climate and supply chain risks, generating the data and awareness needed to prepare for climate impacts [275, 276]. Moreover, the Energy Efficiency Directive (EED) sets binding targets for member states and mandates measures such as annual electricity reductions, mandatory renovation of public buildings, and energy audits for large firms [277, 278]. These directives tie climate policy to sovereignty by reducing dependencies and strengthening supply chain resilience.

Facts

- Climate change could increase European coastal flood damages by more than tenfold by 2100, while droughts may last 2–3 times longer, together threatening ports, mining, and supply chains [265].
- The EU imports over half of its energy, thus remaining dependent on Russian gas, Middle Eastern oil, and US natural gas [267].
- The CSRD and ESRS require firms to disclose climate-related risks, including Scope 3 emissions. These are the indirect emissions from suppliers, transport, and product use that often make up the majority of a company's footprint [275, 276].

Key Drivers

- Strategic autonomy goals push Europe to cut energy use and reduce reliance on external suppliers, exposed by the energy crisis and Chinese rare earth restrictions. Climate directives like the EED and CSRD turn these pressures into binding measures [270, 275].
- Binding EU regulations like the CSRD and EED expand gradually, bringing ever more firms into mandatory climate and supply chain disclosure. By 2028, around 50,000 EU companies and major non-EU subsidiaries will be covered [275, 278, 279].
- By defining clear reduction targets such as the EED's binding 11.7% by 2030, the EU accelerates energy savings and tighter supply-chain controls across the economy [270, 280].

Challenges

- Enforcement gaps weaken EU regulations. Systematic non-compliance, inconsistent penalty regimes, and opaque infringement proceedings erode both credibility and deterrent effect [267]. As a result, the impact of binding rules is reduced.
- Strict regulation can raise compliance overhead and costs for companies, especially in capital-intensive sectors and for Small and Medium-sized Enterprises (SMEs). This discourages investment, slows growth, and shifts operations abroad [269].
- Companies face significant CSRD reporting hurdles: many lack reliable supply chain emissions data and the staff, expertise, or IT systems needed to meet the directive's requirements [281].

Impact on European Digital Sovereignty

Climate directives reinforce Europe's digital sovereignty by reducing dependencies that threaten critical infrastructure. The EED curbs energy demand growth in data centers and AI clusters, lowering import reliance. The CSRD and ESRS institutionalize supply-chain transparency, pushing firms to expose vulnerabilities in ICT hardware, semiconductors, and cloud services. While disclosure rules may remain compliance-driven in the short term, they gradually embed resilience thinking into governance. Overall, by aligning climate policy with sovereignty goals, the EU builds a framework that safeguards infrastructures against climate shocks and strengthens independence from external suppliers.

ENABLING CIRCULAR TECH LIFECYCLES

Recovering Critical Materials From E-Waste and Extending Device Lifespans

Europe's reliance on rare earths and lithium is a strategic vulnerability, with over 90% of processing concentrated in China [266]. These critical materials, essential for GPUs, batteries, and servers, pose not only geopolitical risks but also environmental challenges, further compounding Europe's risk profile [268, 289]. EU sustainability rules, like the EED, raise requirements to reduce the footprint of hardware production. Yet most devices are replaced every 3–5 years, even though many components remain functional for up to a decade [290]. This practice accelerates e-waste, which reached 62M tons in 2022 and is projected to rise to 82M tons by 2030, with only 22% formally recycled [291, 292]. Together, dependence, environmental impacts, and rising waste push Europe toward circular approaches. These approaches enable the recovery of rare-earth magnets and battery materials, potentially covering up to 20% of Europe's rare-earth demand by 2030, while cutting emissions compared with primary raw material extraction [268, 289, 293].

Facts

- Less than 41% of Waste from Electrical and Electronic Equipment (WEEE) is collected in the EU, far below the 65% collection target set by the WEEE Directive [293].
- Rare earth recycling rates in Europe remain below 1%, but research and pilot projects are advancing recovery technologies for materials such as neodymium, dysprosium, praseodymium, and lithium, laying the groundwork for increased circularity in the future [289].
- EU deposit-return schemes can raise return rates for small devices from below 5% today to as high as 62%, significantly increasing available resources for reuse and recycling [293].

Key Drivers

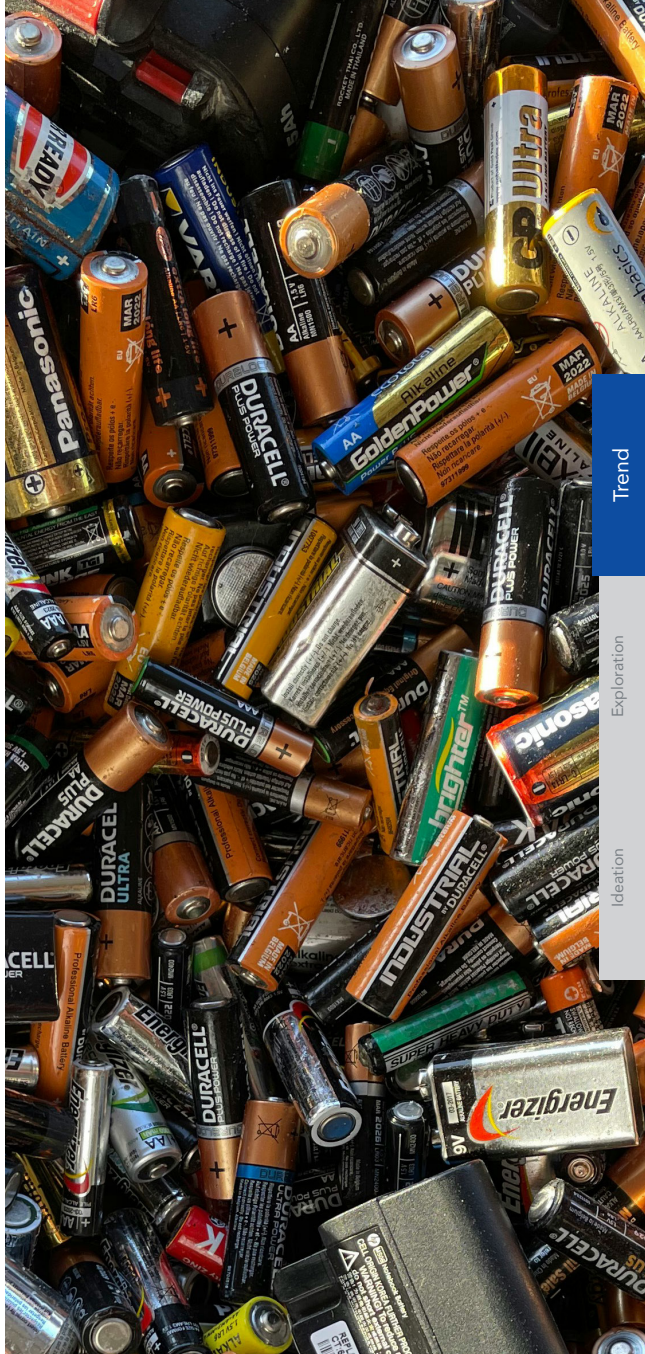
- The Critical Raw Materials Act (CRMA) requires that by 2030, at least 25% of EU demand for strategic raw materials must be met through recycling [268].
- With 90% of rare earth processing concentrated in China, Europe faces supply risks due to export restrictions [289].
- Advances in recycling technology and successful deposit-return pilots show that large-scale circularity of electronics is becoming technically feasible and socially accepted [289, 293].
- The Digital Product Passport embeds data on composition, repair, and recycling, extending product lifetimes, improving recovery of critical materials, and incentivizing circular design [268, 289].

Challenges

- Large volumes of e-waste escape formal collection and recycling as many devices are kept unused in homes and workplaces, while rapid replacement cycles accelerate waste streams [293, 294].
- Disassembly remains technically complex, and many pilot projects are not yet commercially viable. High upfront investment and long lead times for recycling technologies and infrastructure further delay the move to industrial scale [289, 292].
- Chinese firms are expanding into Europe's recycling market, risking external dominance over the very capacity meant to reduce dependence [289].

Impact on European Digital Sovereignty

Circular lifecycles for hardware products can secure critical inputs for batteries, GPUs, and servers that underpin Europe's digital infrastructure. Expanding deposit-return schemes, robotic disassembly, and magnet recycling can turn e-waste into a domestic resource stream, reducing reliance on Chinese rare earth supply and keeping value-added processing in Europe. As an additional benefit, recycling critical materials lowers emissions relative to primary production. In the long term, embedding critical materials recovery and processing in Europe's industrial base will reduce dependence, reinforce competitiveness, and thus strengthen digital sovereignty.



POWERING CLEAN ENERGY

Ensuring Secure, Stable, and Sustainable Power for Next-Generation Data Centers

Europe's digital future depends on two parallel energy goals: building a sustainable power system and ensuring a sufficient, stable supply to meet surging demand. Today, 33% of Europe's electricity still comes from fossil fuels or is imported, leaving critical infrastructure exposed to price volatility and geopolitical risk [296, 297]. While data centers currently account for a modest ~2% share of total electricity use, their demand is projected to grow steeply over the coming decade, driven by AI training and cloud workloads [271]. Without abundant, affordable green power, this growth will be constrained. Moreover, investments in renewable generation, grid storage, and hydrogen systems also enhance the energy resilience of other key sectors, including manufacturing, agriculture, and transportation [298, 299, 300]. Nuclear innovation, including small modular reactors and fusion, offers long-term stability, although most near-term capacity will come from renewables [301]. A diversified, European energy portfolio will shield data centers from external shocks, deliver reliable power, and advance climate neutrality [302, 303].

Facts

- European data centers consumed approximately 50–70 Terawatt-hours (TWh) of electricity in 2023, with projections for 2030 ranging from 160 TWh to nearly 265 TWh, depending on growth and efficiency scenarios [271].
- While nuclear innovation is advancing, large-scale deployment is unlikely before 2035, so most European hyperscale data centers rely on renewables, with wind and solar providing over 60% of the green electricity they procure [296, 302, 303, 304].
- Hydrogen pilots have advanced beyond the lab, as demonstrated by Microsoft's 1.5 MW fuel-cell test powering servers in the US at 250 kW for 48 hours [298, 305]. Europe still lacks comparable large-scale demonstrations, highlighting a gap in zero-carbon backup deployment.

Key Drivers

- Carbon neutrality targets and EU regulations, such as the 2024 Data Centre Sustainability Reporting scheme, make renewable sourcing a compliance obligation rather than a voluntary choice [302, 304].
- Long-term power purchase agreements (PPAs) are a key mechanism to secure and finance low-carbon energy. Microsoft's Nordic wind farm PPAs ensure stable, predictable electricity for its European data centers [303, 304].
- Equinix's >100 MW solid-oxide fuel cell rollout with Bloom Energy shows that mature microgrid and hydrogen solutions are available. By adopting them, Europe can secure resilient, zero-carbon backup power [298, 303].

Challenges

- Building infrastructure for next-generation energy systems is costly and complex, due to high upfront investment, immature supply chains, and the need for significant transmission and distribution grid upgrades [306].
- Regulatory uncertainty and public skepticism about safety, waste, and long-term risks complicate the rollout of advanced nuclear power, slowing commercialization and grid integration [307].
- Intermittency of wind and solar power requires massive investment in storage and balancing capacity. Without it, data centers face exposure to price spikes during low-generation periods [303, 304].

Impact on European Digital Sovereignty

Clean, reliable, and European-controlled energy is a prerequisite for digital sovereignty. Achieving both goals, a sustainable power mix and sufficient, stable capacity, will shield data centers from external price shocks, reduce reliance on non-European suppliers, and help meet climate targets. Reliable electricity underpins cloud computing, AI training, and data-driven innovation, making energy independence a direct enabler of Europe's digital competitiveness. By building next-generation energy infrastructure, Europe can scale its digital economy on its own terms, strengthen resilience against geopolitical risks, and secure long-term strategic autonomy.

GREENING DIGITAL INFRA-STRUCTURE

Decarbonising Networks, Edge, and Data Centres Across Europe's Energy System

The expansion of Europe's digital infrastructure is accelerating, encompassing data centers, telecom networks, and edge nodes. EU data center electricity consumption is projected to increase by ~75% until 2030 and more than double by 2035 [272]. Without major efficiency gains, the sector risks locking in rising energy use that undermines climate targets and inflates operating costs [290]. Energy efficiency, not just cleaner power, is therefore becoming a strategic imperative. Modern optimizations span the stack: next-generation network equipment reduces power per bit, while advanced cooling and low-Power Usage Effectiveness (PUE) designs cut heat waste in large-scale data centers [308, 309]. Edge computing can lower system-wide energy needs by reducing data transport and enabling local load balancing [310]. AI and other computationally intensive workloads can be made less energy-intensive through model optimization and distillation, low-level performance tuning, hardware acceleration, and carbon-aware scheduling [311]. Europe's ability to deliver digital growth without proportional increases in energy use will be a defining test for digital sovereignty [312].

Facts

- EU data center electricity demand will rise from 96 TWh in 2024 to 168 TWh by 2030 and 236 TWh by 2035 [272]. To address this growth, advances in liquid cooling could cut data center energy usage by 15–20% compared to traditional air cooling [309].
- European edge computing capacity is growing at ~21.7% annually, shifting energy use toward distributed micro data facilities close to users [290].
- AI training is resource-intensive, with GPT-3 consuming up to 700,000 L of water, and global AI water use projected to reach 4.2–6.6B m^3 by 2027, more than the annual water withdrawal of 4-6 Denmark [313].

Key Drivers

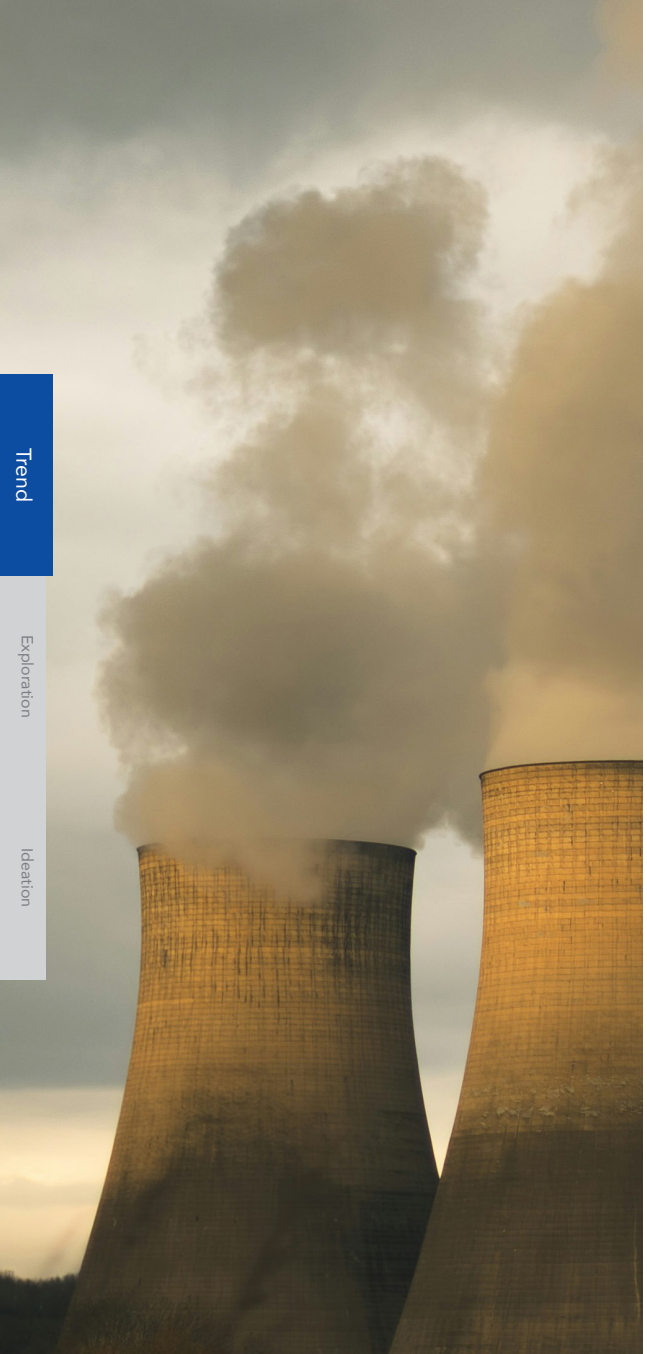
- EU regulations, like the new data center sustainability rating scheme, introduce mandatory efficiency reporting and set measurable benchmarks for PUE, water use, and other resource indicators [314].
- Rising electricity prices and rack power densities exceeding 100 kW make energy efficiency a cost-critical design priority, accelerating the adoption of liquid and immersion cooling technologies, such as Submer, to cut cooling energy demands [315].
- Rapid growth in AI workloads and data traffic drives the demand for model optimization, specialized hardware accelerators, and distributed edge deployment to control energy use at scale [311].

Challenges

- Many data centers already operate near best-practice efficiency, so further energy savings show diminishing returns and become costlier to achieve [316].
- Retrofitting existing facilities with liquid cooling or heat-reuse systems is expensive and often constrained by distance and temperature limits, making upgrades difficult [290, 309].
- The AI race and rising data traffic can outpace efficiency gains, driving higher total energy use despite better technology [313].
- Inconsistent efficiency metrics and reporting make it difficult to compare data center sites and enforce harmonized EU standards [314].

Impact on European Digital Sovereignty

Improving energy efficiency allows Europe to expand its digital infrastructure without a proportional increase in electricity demand, reducing exposure to grid bottlenecks and reliance on non-EU energy imports [272, 290]. At the same time, lower operating costs improve the competitiveness of European cloud and edge providers, helping to retain data processing within the EU. Efficiency gains also reduce local environmental impacts, build public acceptance, and make it easiest to locate new data center capacity domestically [309. Finally, harmonized efficiency reporting and performance standards enable Europe to set global benchmarks, ensuring that future networks, edge nodes, and AI clusters are built with resilience and resource efficiency in mind [312, 314].



REUSING EXISTING IN-FRASTRUCTURE

Leveraging Existing Grid and Utilities to Shorten Delivery Timelines and Lower Embodied Emissions

Across Europe, developers weigh trade-offs between brownfield and greenfield sites for hyperscale data centers and telecommunication hubs. Greenfield projects develop unused land, allowing power, cooling, and layouts to be designed from the ground up. In contrast, brownfield projects convert retired power plants or industrial sites, using existing grid links, substations, and sometimes water infrastructure [272, 317]. This reuse can reduce deployment timelines by 7-10 years [272], while brownfield projects can come online much faster. Reuse also lowers embodied carbon from concrete and steel [318] and often faces less opposition than building on farmland [274]. However, many sites require soil remediation, asbestos removal, or structural upgrades before they can host IT infrastructure and liquid cooling [273, 319, 320, 321]. Ultimately, the decision between greenfield and brownfield lies in total timelines and costs. Greenfield faces lengthy approvals but simpler builds, while brownfield offers faster grid readiness but more remediation risks. Governmental willingness often decides which model delivers sooner and more cost-efficiently [272, 318].

Facts

- Public sentiment tends to favor brownfield over greenfield, e.g., a 2024 UK survey found ~80% positive attitudes to brownfield regeneration [322].
- European grids need ~1.2T EUR in upgrades by 2040. Therefore, prioritizing sites with existing grid capacity helps deliver compute sooner with fewer network reinforcements [323].
- Reusing buildings can significantly reduce embodied carbon, which can account for up to 50% of a data center's lifetime carbon dioxide footprint [318].
- Retired coal and gas plants owned by Engie, RWE, and Enel are already being redeveloped into data centers, offering the first pilot projects [317, 324].

Key Drivers

- Surging demand for sovereign cloud and AI makes rapid deployment essential, as delays risk capacity shortages, higher costs, and reliance on non-EU providers [272].
- EU incentives for remediation and site regeneration, such as the ERDF and LIFE programmes, improve the financial viability of brownfield developments [273, 325].
- Community support is typically stronger for revitalising industrial land than for building new sites on farmland or near sensitive landscapes, provided that water use, noise, and traffic impacts are carefully managed [274].

Challenges

- Many brownfield sites require costly remediation, which can be particularly challenging when involving strict safety protocols and specialised disposal [273, 319].
- Legacy site layouts may not support high rack densities or advanced liquid cooling without major structural works, e.g., ceiling heights, raising retrofit costs and limiting long-term scalability [320, 321].
- Slow and fragmented permitting across multiple agencies, combined with unclear liability rules, can negate the brownfield time advantage [272, 273, 325].

Impact on European Digital Sovereignty

Prioritising brownfield reuse lets Europe expand sovereign cloud and AI infrastructure faster while keeping operations under EU law through data residency and security controls. This approach shortens grid connection times, avoids the production of thousands of tons of concrete and steel, and aligns growth with EU climate targets [318]. Because industrial sites face less community opposition, it also strengthens the political and social backing for sovereignty initiatives [274]. Together, these benefits reduce reliance on non-EU providers, limit extraterritorial access risks, and give the EU greater control over technical and security standards. A balanced mix of brownfield reuse and targeted greenfield builds ensures long-term capacity and resilience [325].

EXPLORATION

In the upcoming chapter, the outcomes of the process for validating hypotheses and problem statements are explored. This phase primarily revolves around the discovery of white spaces and opportunity areas relevant for *The Future of Digital Sovereignty*. By clustering the topic, findings are distilled into five key opportunity spaces, and the most critical problems and opportunities within the chosen domain are identified. The exploration phase places a priority on the testing and re-evaluation of hypotheses with expert insights, alongside an examination of the existing landscape to pinpoint selected players.

SMART INFRASTRUCTURE

INFLUENCING THE FUTURE OF DIGITAL SOVEREIGNTY

Enabling Smart Energy Consumption
Building Next-Generation Connectivity Systems
Advancing Edge AI Applications

Superblocks in Barcelona, Spain

Adrian Stoica 
Andriani Nikolaou 
Charlotte Schöllkopf 
Gjergj Kukaj 
Karolina Wick 
Malte Oberhoff 

SMART INFRASTRUCTURE

Strengthening the Backbone of European Digital Sovereignty

Europe's digital infrastructure is entering a transformative era. Data centers, mobile networks, and edge devices are increasingly critical to economic competitiveness, innovation, and societal resilience. Yet, this growth brings challenges as well. Data-center electricity demand is set to double by 2030, renewable energy introduces grid volatility, traditional mobile networks remain rigid and incomplete, and cloud-centric AI struggles to meet the latency, privacy, and autonomy needs of emerging applications [328, 329, 330]. Addressing these challenges is essential for a sovereign digital infrastructure while advancing Europe's green energy and technology leadership.

First, Europe must reimagine energy consumption. By leveraging data centers as flexible energy assets, this challenge can be turned into a solution. Dynamically shifting computing workloads helps to stabilize power grids and maximize renewables. This capability transforms data centers from energy consumers into active grid partners, creating strategic value beyond their computing function. This approach not only cuts costs but also strengthens the strategic case for European sovereign data centers [331, 332]. Building on this, the next pillar is next-generation connectivity. Resilient, open networks are crucial. Standards like Open RAN and integrated satellite systems promise to close coverage gaps and reduce supplier dependency. This creates a robust foundation for essential services and fosters vital multi-vendor interoperability [333, 334]. Finally, with powerful networks in place, intelligence moves to the edge. By distributing intelligence closer to where the data is generated, Edge AI reduces latency, strengthens privacy protections, and enhances resilience against network disruptions. Edge AI brings processing directly to devices, enabling faster, more private decisions for applications from autonomous vehicles to healthcare. This shift is crucial for meeting the real-world needs of emerging applications while reducing reliance on centralized cloud systems [7, 335].

Together, these three pillars illustrate a holistic approach to Europe's smart future: energy-aware, connected, and intelligent infrastructure that enhances operational efficiency, environmental sustainability, and technological sovereignty. For businesses, policy-makers, and researchers, this convergence represents a substantial opportunity to innovate and lead in the next generation of computing and communication technologies.

ENABLING SMART ENERGY CONSUMPTION

Using the Flexible Energy Demand of Data Centers to Enhance Grid Stability

Data centers are driving a surge in global electricity demand. They currently consume 1.5% of global power, with consumption expected to double by 2030 [328]. This growth coincides with a critical challenge: renewable energy has made grids more volatile, as solar and wind output fluctuates and spikes with weather patterns. Maintaining grid stability now requires energy consumption that can adapt to these fluctuations. Data centers offer a unique advantage in this regard: unlike traditional industrial loads, computing tasks can be scheduled for specific times or relocated to different sites [331, 336]. This enables demand shifting on a large scale: tasks can be moved to times with higher energy availability or to locations with cheaper or cleaner power [332, 337].

However, steering computational workloads is complex, requiring dynamic allocation of processing capacity across distributed facilities. As electricity costs increasingly dominate datacenter operations, the business case for demand shifting strengthens. With computing power becoming a low-margin commodity, flexible energy consumption will be essential for building cost-competitive sovereign data centers [338]. For Europe, this approach not only enhances the competitiveness of sovereign data centers, but also helps stabilize the power grid and advance the green energy transition.

> “I think it will be ‘common sense knowledge’ in just a few years that AI data centers are grid stabilizers. We’d love to do it in more places.”
>
> Urs Hölzle, Google [339]

Selected Players

terralayr · ACCURE · Ekko Sense · EnBW · uplight · Entrix · submer · GridBeyond · STATERA · QARNOT

BUILDING NEXT-GENERATION CONNECTIVITY SYSTEMS

Open Interoperable Satellite-Terrestrial Networks for Resilient Services

Mobile networks have traditionally been built as closed systems, with all components coming from a single vendor. Yet, this has slowed innovation and made switching extremely difficult [329]. The Open Radio Access Network (O-RAN), however, is changing this by establishing common standards that allow equipment from different manufacturers to interoperate. This enables network operators to mix and match components and reduce dependence on a single vendor. While global testing centers are validating this interoperability, seamless multi-vendor operation remains challenging [340].

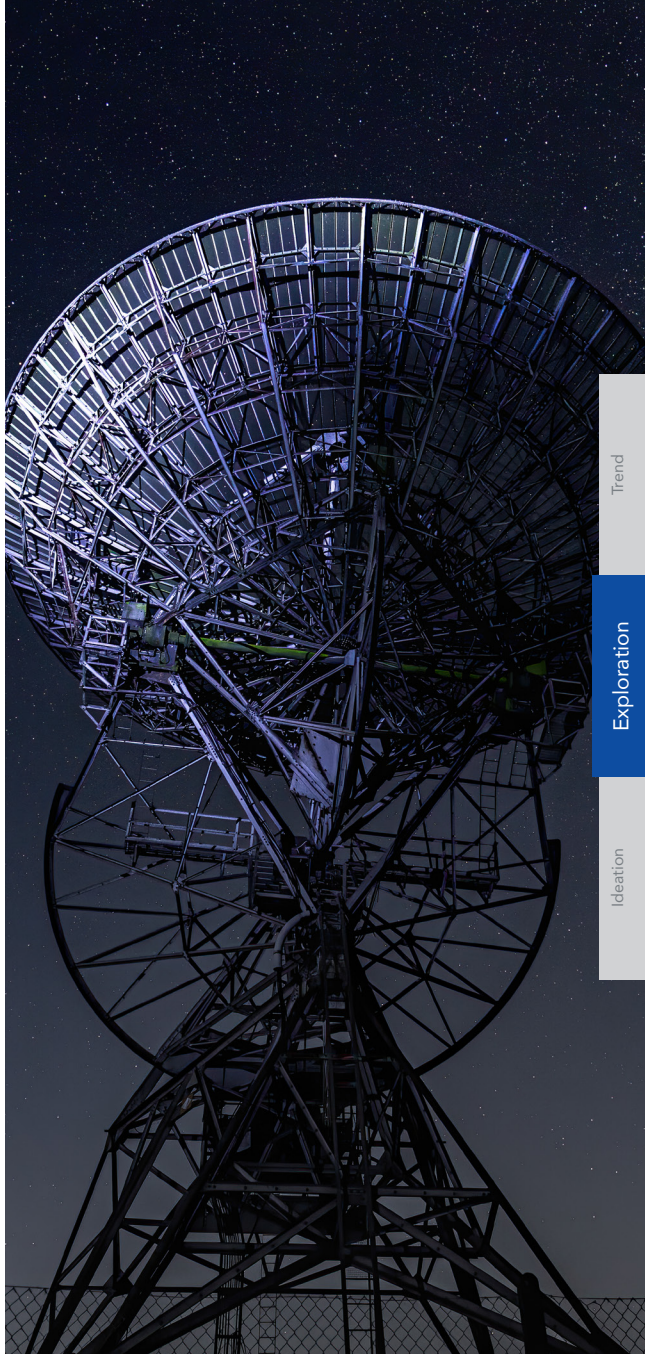
Meanwhile, current mobile networks only function where cell towers exist, leaving gaps in rural areas, oceans, and remote regions. New standards from the 3rd Generation Partnership Project enable satellites to connect directly to 5G phones, with broader integration planned [333]. For 6G, the International Telecommunication Union envisions combining ground and satellite networks [341]. Moreover, Europe's Union Secure Connectivity Programme funds its own satellite constellation to keep connectivity under European control and close coverage gaps [342].

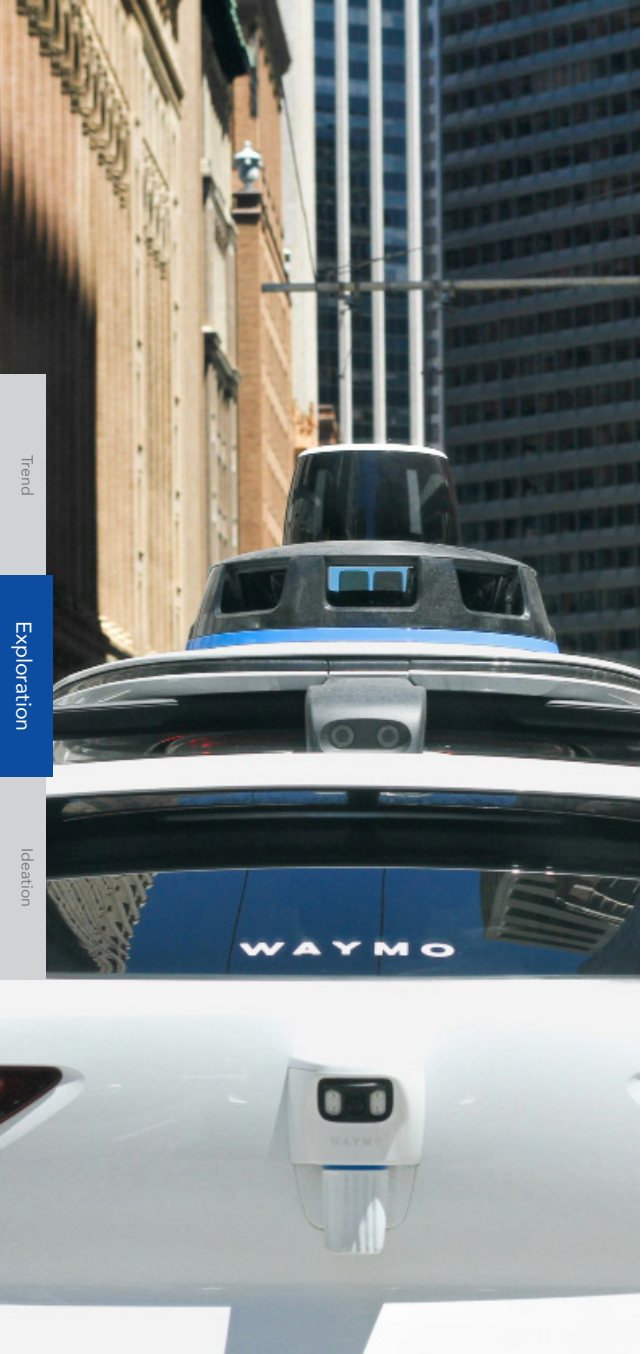
However, a simple method to integrate these networks seamlessly is lacking. Many projects succeed in pilots but fail at scale. A shared application layer could turn these standards into reliable services for public safety, transport, maritime, and energy, while reducing reliance on single suppliers [334].

> "Open RAN is real, performing, and moving forward; there is no way back."
>
> Dimitris Mavrakis, ABI Research [343]

Selected Players

IRIS²
astrolight
ERICSSON
SATELIOT
Space · Connecting · 5G IoT
is-wireless
firecell
astrocast
SES
your satellite company
EchoStarMobile
emnify





ADVANCING EDGE AI APPLICATIONS

Enabling Smarter and Private Devices through Edge AI

Integrating AI in areas like robotics requires a paradigm shift from traditional cloud computing to more responsive and robust solutions. While the cloud offers immense compute power, its inherent latency and bandwidth limitations are critical barriers for real-time applications [330]. Edge computing solves this by moving computation directly to the data source, enabling on-site processing for faster response times and enhanced data protection [7]. In combination with edge hardware becoming more powerful, the market for Edge AI is expected to more than triple by 2030 [344, 345].

This development unlocks transformative opportunities across industries. In manufacturing, it enables real-time defect detection on assembly lines, preventing costly production errors. For autonomous vehicles, it facilitates instantaneous decision-making, essential for navigation and safety [346]. In healthcare, it allows for continuous patient monitoring with strict data privacy, as sensitive information never leaves the device [335]. Furthermore, by deploying small, efficient AI models directly on edge hardware, companies can build more intelligent and autonomous products while significantly reducing their dependence on external cloud infrastructure, leading to greater operational resilience and efficiency.

> “This is going to be the decade of autonomous vehicles, robotics, and autonomous machines.”
>
> Jensen Huang, CEO of Nvidia [347]

Selected Players

WAYMO, Microsoft, amazon, NVIDIA, Google, HUAWEI, Telit Cinterion, SUPERMICRO, Rockwell Automation, BOSCH

RESILIENT RESOURCE CYCLES

INFLUENCING THE FUTURE OF DIGITAL SOVEREIGNTY

Alternative Sourcing of Raw Materials
Material Circularity as a Sovereignty Lever
Turning Data Into Europe's Strategic Asset

Garzweiler Mine in North Rhine-Westphalia, Germany

Anjella Klaiber 
Hanano Shiga 
Jakob Limmer 
Jonathan Mäusle 
Katy Grossman 

RESILIENT RESOURCE CYCLES

Building Interconnected Resource Cycles to Strengthen Physical and Digital Value Chains

Europe's future competitiveness and autonomy are tied to critical raw materials. Yet, the EU relies heavily on a limited number of external suppliers, creating significant supply risks. Based on the European Commission's 65% import concentration threshold, China exceeds concentration limits for bismuth, cobalt ore, magnesium, manganese, and strontium, Turkey for borates and feldspar, and the United States for beryllium [348]. This underscores structural vulnerabilities in Europe's supply chains.

The EU tackles these vulnerabilities with the CRMA. It aims to develop a European value chain for critical raw materials and diversify the import routes that bring these minerals into the EU. The CRMA's push for a domestic value chain aims to secure a supply of 10% of the EU's raw materials and refine 40% of these by 2030. Diversification of imports seeks to reduce reliance on a few suppliers by supporting new critical raw materials projects in emerging economies, and providing funding in exchange for prioritized access to these resources [349].

Securing new sources of raw materials is not only an economic and political challenge but also a scientific one. Various projects spearheaded in the EU illustrate the growing technical feasibility of material extraction and recovery methods. Particular examples include bioleaching, which uses microorganisms for metal extraction, recycling of lithium batteries, or upcycling mining waste to construction materials [350, 351]. These efforts form part of a broader strategy where Europe identifies new ways of material procurement. Instead of exclusively relying on imports or domestic value chains, another alternative for Europe is to invest in circular resource cycles. While the EU used 11.8% of recycled materials in 2023, its Clean Industrial Deal aims at doubling this amount to 24% by 2030 [352, 353]. The trajectory towards that goal is not very promising, given the use of 10.7% of recycled materials in 2010 [352]. This is mainly due to product designs often not being optimized for circularity, and information on material composition frequently lacking. At the system level, effective collection and recycling of waste requires appropriate facilities and technologies, a task made more difficult by the EU's high resource consumption [354]. Complementing this, improving product design, collection, and recycling can maximize the value recovered from resources.

Data plays an increasingly important role in the successful functioning of supply chains [355]. To fully realize sovereign resource cycles, Europe must retain control over this digital resource, ensuring that data infrastructures remain within its regulatory and operational domain [356]. As a result, turning data into a strategic asset is one of the ways in which Europe can drive innovation and sovereignty. Together with alternative sourcing and material circularity, this approach strengthens Europe in physical and digital domains.

ALTERNATIVE SOURCING OF RAW MATERIALS

Leveraging Innovative Mining Technologies and Material Discovery

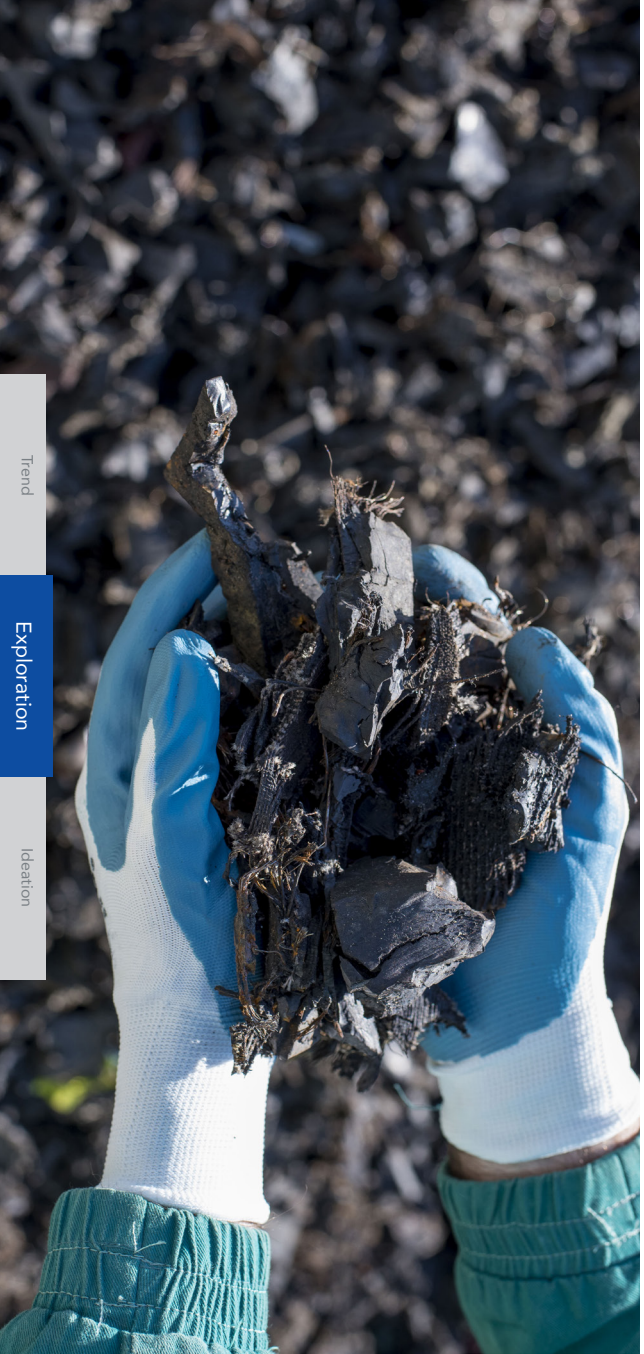
90% of raw material extraction and 60% of processing occur outside the EU, with China as the dominant supplier [357]. To reduce its dependency, Europe must diversify its raw material sources instead of relying on third-country suppliers. This includes commercializing innovative mining technologies and harnessing domestic resources through approaches such as direct lithium extraction, or in-situ bioleaching, and extraction of metals using microorganisms directly from the ore vein [358, 359]. These methods could be more sustainable than conventional methods [360, 361].

Meanwhile, increased R&D investment for alternative materials is opening promising pathways. For example, substituting lithium with sodium in batteries has proven to be a viable and more cost-effective solution without major performance drawbacks [362]. Emerging tools such as computational chemistry and AI-driven material discovery can accelerate the search for sustainable substitutes. AI models like GNoME have demonstrated that new materials can be predicted, validated, and synthesized within weeks [363]. Through innovation in mining technologies and alternative material discovery, Europe has the potential to enhance its resilience and deliver on the objectives outlined in the Critical Raw Materials Act [364].

> “The environmental cost in the production of AI tools, ChatGPT, [and other] things we use in our daily lives is inherently material in nature and all of them [come at a high] cost.”
>
> Dr. Mohammad Amir Anwar, University of Edinburgh [365]

Selected Players

Enpal. RWE EnBW 1KOMMA5° thermondo Ørsted VATTENFALL enercity positive energie ERG EVOLVING ENERGIES eni



MATERIAL CIRCULARITY AS A SOVEREIGNTY LEVER

Shifting From a Linear to a Closed-Loop Material Industry

The pursuit of a circular economy offers Europe a strategic chance to enhance sovereignty and cut dependence on external resource providers. The current model, which relies on extracting raw materials and disposing of waste, creates a major vulnerability to foreign supply chains. This is reflected in Europe's low recycling rate of 8.3% for critical materials [366]. This shortfall drives import reliance and leaves the continent far from its goal of a 24% recycling rate for critical raw materials by 2030 [353]. Additionally, methods like automated waste sorting exist but are less important for reaching circularity goals.

The real sovereignty potential lies in higher-level strategies of refusing and reducing material use upfront [367]. These strategies are still under-emphasized by companies, even though they deliver the largest environmental and economic gains by decoupling growth from resource consumption [368]. By innovating in durable design for disassembly and fostering product-service systems, where businesses keep ownership of products and customers only pay for their use or the service they provide, Europe can mitigate supply-chain risks [369, 370]. This shift from reactive recovery to proactive reduction is a foundational step toward a more resilient, self-sufficient, and competitive European economy.

> "Legacy players are heavily investing in material circularity solutions, and strong vertical integration activities can be expected in the near future."
>
> Nina Odefey, Lakestar

Selected Players

CYLIB, Hydrovolt, ATEA, tozero, FAIRPHONE, interzero, Foxway, Atlantic Copper, Aurubis, umicore

TURNING DATA INTO EUROPE'S STRATEGIC ASSET

Building a Sovereign, End-to-End Data Ecosystem to Drive Innovation

Europe relies heavily on non-European providers for various parts of the data value chain. This dependency stems from underinvestment in scalable European alternatives and problems in aligning data-driven innovation with privacy regulations. As data becomes a strategic asset underpinning competitiveness in the digital sector, Europe must transition from regulating data to actively leveraging it for economic resilience [1, 371].

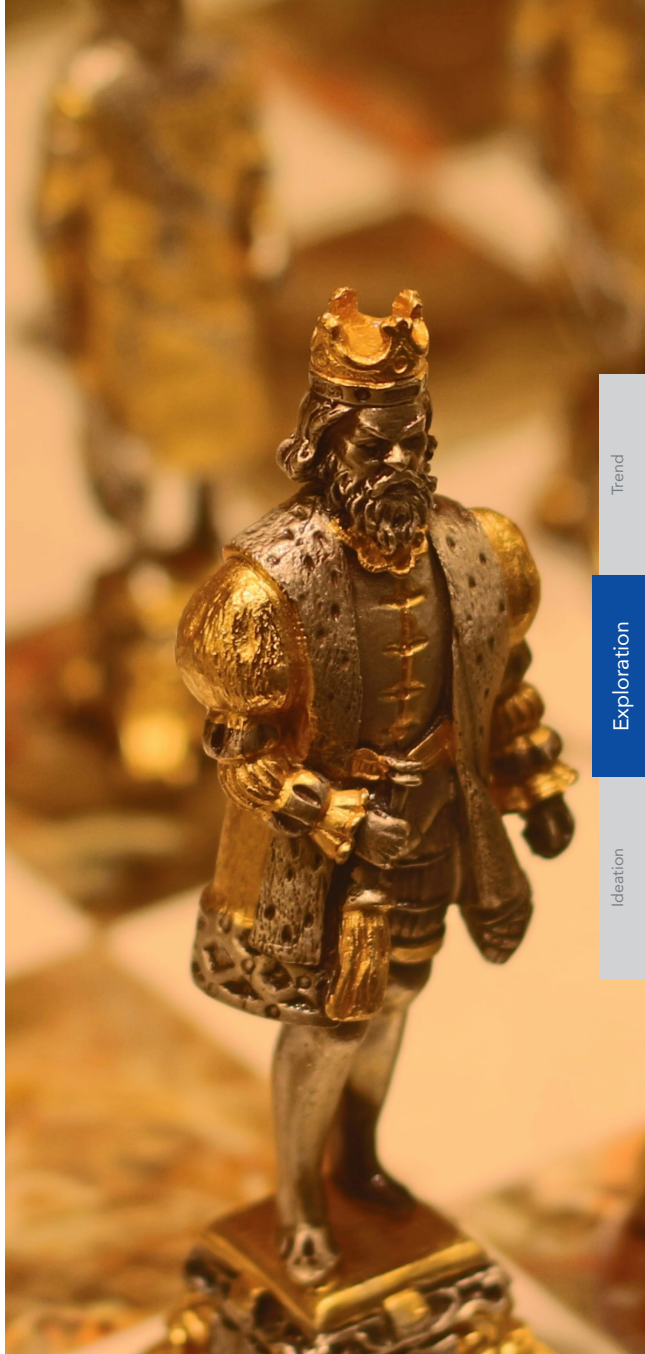
Without intervention, European companies risk becoming locked into foreign ecosystems and losing control over value creation. US providers now dominate the European cloud market with a 70% share. Meanwhile, European providers have seen their share fall from 29% in 2017 to just 15% in 2022 [372].

Conversely, building a robust European data ecosystem that brings together actors for trustworthy data use can unlock innovation and enable industry-wide collaboration [373, 374]. By empowering local providers and creating competitive advantages in privacy-preserving data solutions, Europe's rich data assets can become a driver for sustainable growth. Ensuring secure, ethical, and cross-border data use will be essential for this goal [373]. Ultimately, treating data as a strategic asset is central to strengthening Europe's digital sovereignty.

> "Value creation from data, and the use of [...] AI will change many, if not all, sectors of the economy in a very short time."
>
> Thomas Hahn, BDVA [375]

Selected Players

soffico · European Environment Agency · Copernicus Europe's eyes on Earth · HETZNER · Schneider Electric · ALEPH ALPHA · eurostat · celonis · Collibra · DuckDB



SECURING EUROPE

INFLUENCING THE FUTURE OF DIGITAL SOVEREIGNTY

Deploying Autonomous Systems in Defense
Shielding Critical Systems
Pioneering Independent Space Technologies

Lovrjenac Fortress in Dubrovnic, Croatia

Benedikt Albertsen 
Danit Niwattananan 
Niklas Reminger 
Nikolas Keller 
Salan Isaqzoi 

SECURING EUROPE

Advancing Autonomy in Defense, Infrastructure, and Space

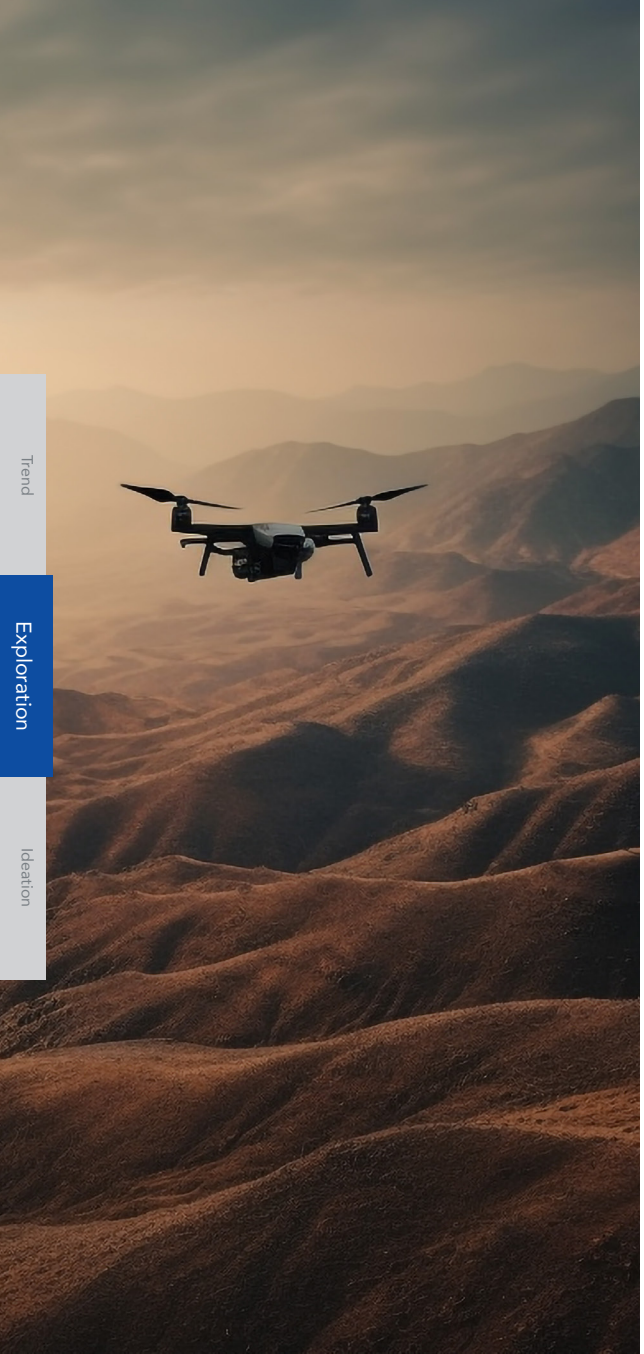
Technological capabilities are increasingly decisive for Europe's sovereignty [376]. Modern conflict and hybrid threats show that control of autonomous platforms, resilient infrastructure, and access to space now shape security outcomes as much as traditional military strength [377, 378]. Unmanned systems alter the course of wars, cyberattacks disrupt daily life and critical services, and satellites determine whether governments and militaries can communicate, navigate, and detect threats [379, 380, 381, 382]. In each of these areas, dependence on external providers exposes vulnerabilities, while strengthening European capabilities creates both strategic resilience and economic opportunity [376, 383].

The first domain where this becomes visible is autonomous defense systems. The war in Ukraine highlights how unmanned platforms provide decisive advantages by extending situational awareness, accelerating decisions, and limiting risks to personnel [379, 380, 384]. Europe's market in this sector is expected to grow, but today it relies heavily on foreign providers [376, 385]. This dependence creates strategic risks if supply chains are disrupted or export restrictions are applied [377]. Developing next-generation European systems is therefore essential to safeguard operational autonomy and also to capture industrial value in a rapidly expanding global market [376, 383].

Autonomous defense systems, however, do not function in isolation. They depend on the stability of the environment in which they are deployed. Europe's critical infrastructure, which includes energy, transport, water, and communications, is exposed to systemic threats [381, 386]. Modern cyberattacks can bring down legacy systems, while climate change drives extreme weather that puts infrastructure under stress [378, 387, 388]. Once again, in both cases, reliance on outdated or externally controlled technologies amplifies the risks [389]. Addressing them requires tools to reduce known vulnerabilities and apply security-by-design principles in all infrastructure modernization and development projects [381, 386].

Critical infrastructure was once defined mainly by systems on the ground, but it now increasingly relies on space-based assets [390]. These space systems include, for example, satellites that provide navigation, secure communication, reconnaissance, and missile warning functions [382, 390]. Europe, however, remains strongly dependent on external powers, most often the US, to access these services [386, 391]. With launch costs falling and new commercial opportunities emerging, Europe now has both the need and the chance to strengthen its role [392, 393].

Collectively, autonomous defense, resilient infrastructure, and space capabilities form an interdependent chain of systems [376]. A weakness in one can undermine the others, while strengthening each reinforces the whole [376]. As a result, progress in these domains will shape the future of Europe's technological sovereignty [376].



DEPLOYING AUTONOMOUS SYSTEMS IN DEFENSE

Securing Europe in the Age of Unmanned Warfare

Unmanned systems are transforming modern warfare, as demonstrated in recent conflicts, such as the Russia-Ukraine war. These systems provide strategic advantages through enhanced situational awareness, faster decision cycles, and reduced risk to personnel [379, 394]. Consequently, this transformation is driving significant market growth, with Europe's unmanned systems sector projected to grow by 8.5% annually from 5B USD in 2024, potentially capturing 25% of the global defense market share by 2030 [385].

However, Europe's dependence on foreign technology creates strategic vulnerabilities. The current reliance on systems from foreign powers leaves European forces vulnerable to supply chain disruptions and potential technology restrictions [377, 383]. This dependency stems from decades of underinvestment in indigenous defense capabilities. It has become increasingly problematic as traditional alliances grow more transactional, where a partner's strategic priorities or export controls can directly limit European operational autonomy [395].

This opens up the space for European-made solutions, such as next-generation drones and autonomous platforms, which are crucial for achieving strategic sovereignty. By building domestic capabilities, Europe can secure its defense autonomy while capturing economic value in this growing global market, ultimately strengthening both its security and industrial competitiveness.

> "The thing that is so powerful about autonomy is that you can clearly show your adversaries that you have weapons that do not cost all that much money and that don't cost human life."
>
> Palmer Luckey, Anduril [396]

Selected Players

BOEING · L3HARRIS · Helsing · QUANTUM SYSTEMS · ANDURIL · Raytheon · NORTHROP GRUMMAN · RHEINMETALL GROUP · Palantir · LOCKHEED MARTIN

SHIELDING CRITICAL SYSTEMS

Critical Infrastructure Requires Solutions Against Growing Systemic Threats

Critical infrastructure systems are increasingly vulnerable to a convergence of cyber, physical, and climate-related threats [378, 381]. This interconnection means that a single event, such as a successful cyberattack on an energy grid or a major climate disaster, can trigger cascading failures across economies and societies [386, 397].

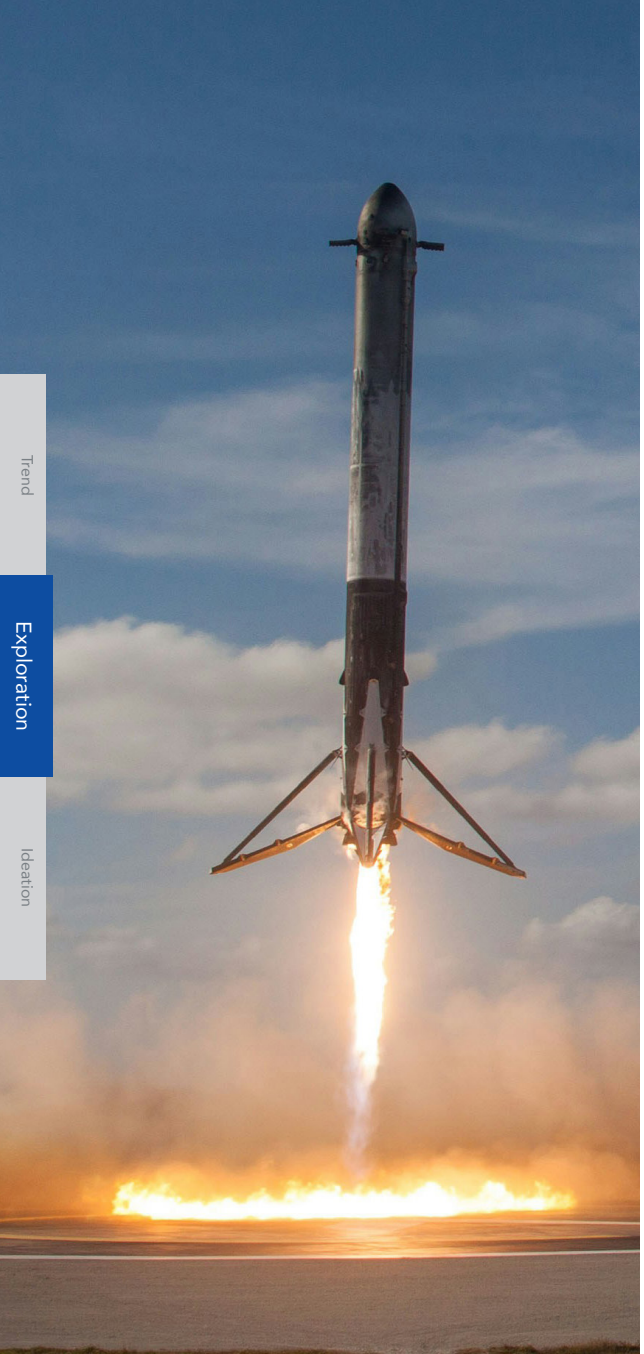
Two underlying conditions fundamentally drive this heightened risk. The first is the widespread presence of legacy infrastructure. These decades-old systems contain inherent vulnerabilities because they were engineered long before modern cybersecurity threats emerged [381]. Secondly, climate change acts as a threat multiplier, exposing fragile infrastructure to extreme weather events, including floods, wildfires, and heat waves [388, 398].

An effective defense requires a coordinated approach addressing both current and future risks, such as upgrading current systems with better monitoring to mitigate known vulnerabilities. It also involves making infrastructure resilient to climate threats using predictive tools enabled by digital twins [386]. The foundation of this effort is building security into new projects from the beginning, creating sustainable protection instead of relying on perpetual repairs [399, 400].

> “In today’s interdependent and interconnected world, the protection and security of our cyber and physical infrastructure requires the concerted efforts of public and private partners around the globe.”
>
> CISA International Strategic Plan [401]

Selected Players

SIEMENS, Fraunhofer IESE, Securitas, WORLD SENSING, CISCO, THALES, Blecon, DARKTRACE, CROWDSTRIKE, IBM



PIONEERING INDEPENDENT SPACE TECHNOLOGIES

Seizing the Launch Window for Europe's Space Sovereignty

Europe's access to earth observability, secure communications, navigation, and missile warning systems still comes largely from external providers, especially the US. These functions are essential in times of stability as well as crisis, yet in Europe they remain hindered by fragmented investment and slow procurement cycles [391]. Traditionally, dual-use programs such as Galileo have been prioritized over space missions in terms of their value to the supply chain, as well as for security and defense purposes [390].

This balance is now shifting, driven by sharply lower launch costs that are transforming the global space landscape. For example, the cost of delivering one kilogram into orbit has been reduced by 90% partly due to the use of reusable rockets [392]. Looking ahead, Europe must seize the opportunity to strengthen its own independent space capabilities. At a time of possible US disengagement, Europe cannot afford to remain underdeveloped. Continued reliance on external systems would leave Europe vulnerable in areas such as communications and intelligence, deepening its dependence on foreign powers [391, 402].

To address this, investing in a robust portfolio of European space assets offers wide-ranging advantages. Beyond immediate defense applications, innovations such as in-orbit semiconductor manufacturing, space-based data centers, and space mining could lead to the creation of new industrial sectors and cross-sectoral goals, such as sustainability targets [393, 403, 404].

> "The next industrial revolution will not be on Earth, it will be in orbit."
>
> Matthias Spott, LEOconomy [393]

Selected Players

isar aerospace · ICEYE · rocket orbit · POLARIS Raumflugzeuge · ThalesAlenia Space · SPACE FORGE · ispace · AIRBUS DEFENCE & SPACE · SPACEX · ASTROFORGE

NURTURING HUMAN CAPITAL

INFLUENCING THE FUTURE OF DIGITAL SOVEREIGNTY

Hyper-Personalizing Digital Literacy Education
Connecting Talent Clusters and Ecosystems
Retaining Talent by Enabling Mobility

University of Oxford, England

Ammar Idriz 
Joe Lammers 
Joseph Gawlik 
Linnea Brand 
Tarak Amouri 

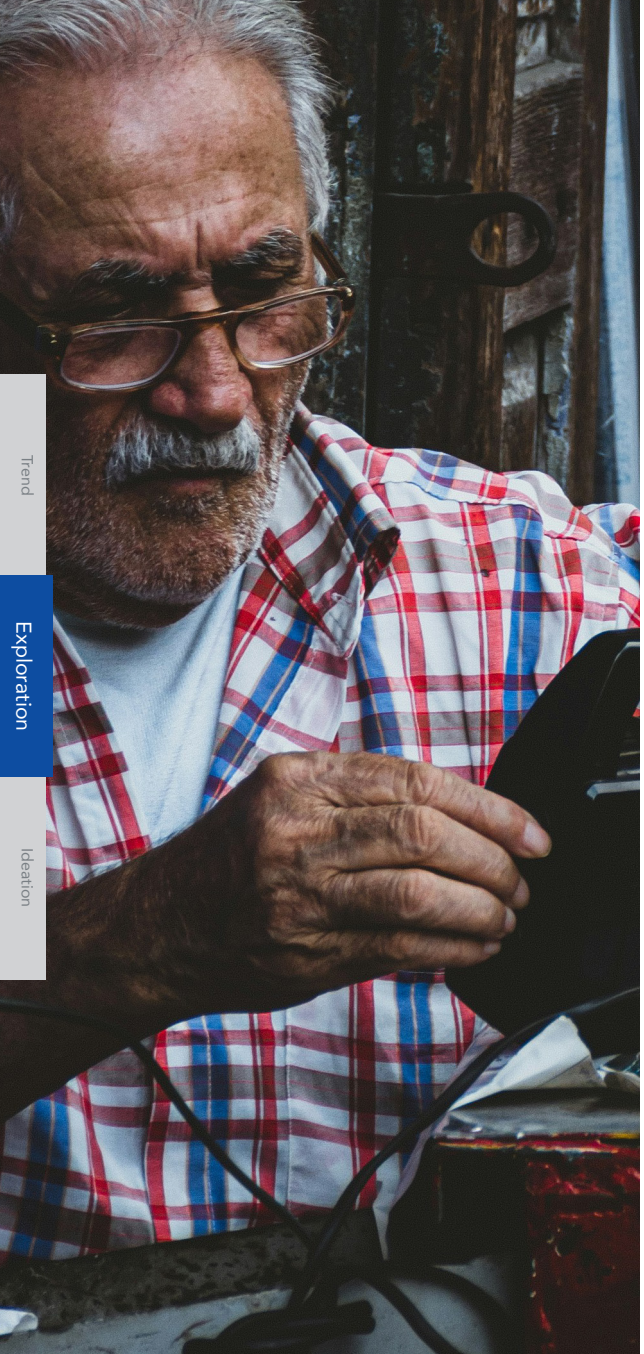
NURTURING HUMAN CAPITAL

Strengthening Europe's Talent Pipeline With Adaptive Learning and Connected Ecosystems

Europe's ambition to become a global digital leader depends on a critical foundation: its people. To achieve true digital sovereignty, the continent must cultivate a workforce that is not only highly skilled but also capable of transitioning across roles, sectors, and borders. Yet a significant human capital gap threatens this goal. Europe faces a pressing shortage of ICT specialists and a broader deficit in the advanced digital literacy that citizens need to thrive, innovate, and participate securely in a data-driven society [405, 406]. This challenge is compounded by a fragmented innovation landscape and systemic barriers that impede Europe's ability to attract and retain top global talent [407, 408]. Closing this gap requires a coordinated strategy that builds talent at every experience level.

The urgency is heightened by accelerating technological shifts. Artificial intelligence, quantum computing, and cybersecurity demands are reshaping the skills required in almost every industry. Without decisive action, the divide between advanced hubs and lagging regions will widen, leaving Europe dependent on external expertise and vulnerable to talent outflows [409]. The stakes are not limited to economic performance. They extend to democratic resilience, social inclusion, and Europe's ability to set global standards in the digital sphere.

In practice, closing the gap requires action in the three domains of skills, ecosystems, and mobility. Across these categories, a common thread emerges: when know-how is scattered across member states, projects struggle to reach critical mass, duplication rises, and time-to-market slips [410]. Hyper-Personalized Digital Literacy illustrates this shift by moving beyond static curricula toward adaptive learning that adjusts to a learner's knowledge level, pace, and style. This equips citizens of all ages to navigate AI, assess information critically, and participate in the digital economy. Connected Talent Ecosystems reflect the same principle in innovation by linking Europe's strong but isolated hubs into cross-border networks that amplify spillovers and scale breakthrough research. Frictionless Talent Mobility completes the picture by ensuring that once skills and ecosystems align, individuals can seamlessly move, settle, and build long-term careers across Europe. By executing this integrated vision, Europe can transform its human potential into tangible digital sovereignty and lasting global competitiveness. Adaptive skills feed vibrant ecosystems, ecosystems thrive when talent circulates, and mobility ensures Europe's best minds contribute where they are most needed. Only through this virtuous cycle can Europe convert its diverse human capital into the collective strength required to lead in the next digital era.



HYPER-PERSONALIZING DIGITAL LITERACY EDUCATION

Equipping Citizens with Digital Literacy Skills for an AI-Driven Economy

Europe's digital resilience is undermined by a widespread inability to grasp the core concepts of technologies such as AI [75]. This skills gap affects all age groups, leaving those with limited understanding vulnerable to disinformation, excluded from essential services, and at a severe disadvantage in the job market [411]. This not only hinders innovation but also actively threatens strategic autonomy, as citizens cannot effectively use, question, or shape the technology that governs their lives [412].

The solution is not another generic online course, but a fundamental shift from static, one-size-fits-all training to learning that is as dynamic as the technology itself. Most initiatives such as corporate training programs remain fragmented and fail to keep pace with change [413].

The emerging opportunity lies in creating inclusive, personalized learning ecosystems. This means replacing outdated curricula with adaptive education tailored to an individual's proficiency, pace, and preferences. By making digital skills accessible at every stage of life, Europe can close the skills gap. This simultaneously strengthens democratic resilience and supports technological independence by cultivating a population capable of building and adopting European alternatives to global platforms.

> "Artificial intelligence enables the next generation of education tools as we can develop hyper-personalized learning tracks for every individual."
>
> Nina Odefey, Lakestar

Selected Players

gloat · codecademy · edX · LinkedIn Learning · KIDE SCIENCE · OBRIZUM · Kahoot! · udemy · EDURINO · coursera

CONNECTING TALENT CLUSTERS AND ECOSYSTEMS

Uniting Europe's Fragmented Innovation Ecosystems

Europe's potential for digital sovereignty is undermined by its fragmented innovation landscape. While strong hubs in AI, semiconductors, and cloud computing exist, they are often siloed by national priorities, divergent regulations, and market barriers [414, 415]. This "regulatory jungle" prevents these clusters from linking into a single, powerful digital space where data, talent, and capital move freely across borders [416]. The consequence is a chronic inability to turn world-class research into globally competitive products and scale companies within Europe [417]. Parallel yet disconnected clusters limit the essential spillovers and network effects that drive true innovation [418].

The central opportunity is not to create more isolated hubs, but to strategically connect the ones that already exist [419]. Models like Stockholm's scale-up "flywheel," Berlin's cultural hub, and Munich's innovation factory show the power of concentrating talent, capital, and infrastructure [420]. The emerging opportunity is to replicate this success at a continental scale.

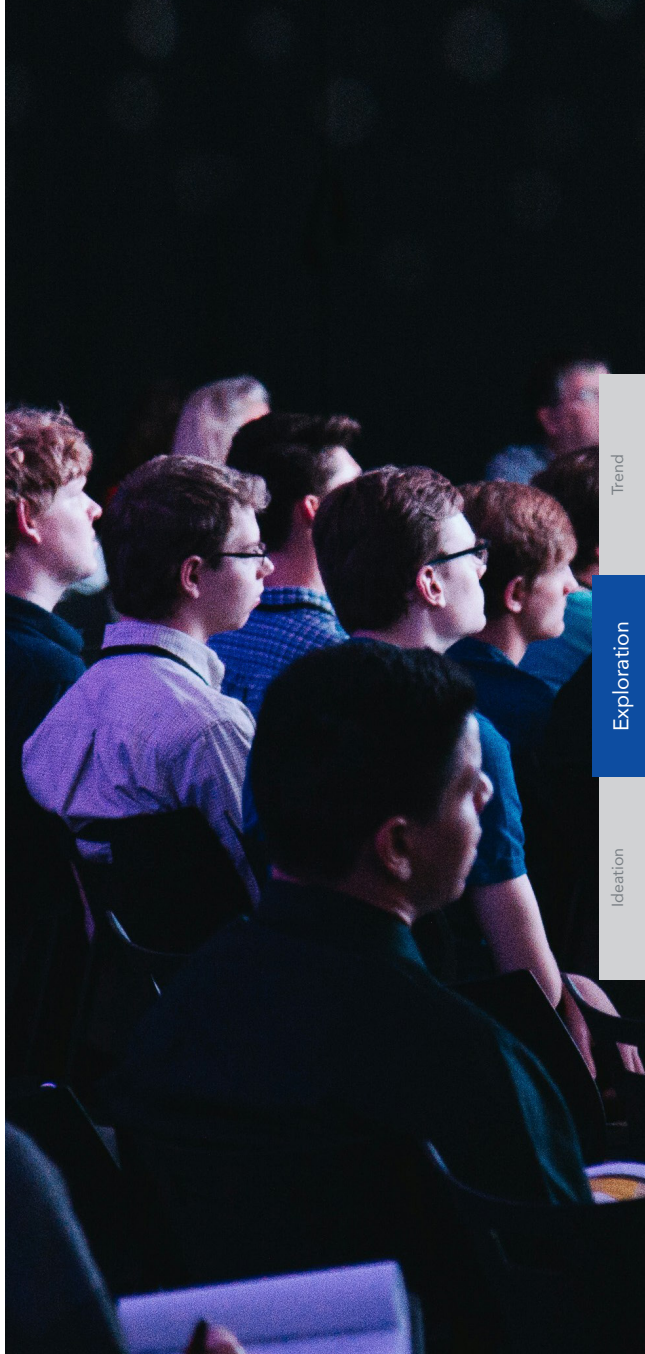
Overcoming this fragmentation demands a pan-European platform that connects these clusters. By building stronger networks to match ventures, capital, and skilled professionals across borders, Europe can accelerate high-growth sectors. This would transform isolated pockets of excellence into a unified, competitive innovation space, maximizing spillovers and finally strengthening Europe's digital sovereignty.

> "Lasting innovation ecosystems are not built through top-down directives. They must be cultivated from the bottom up, empowering firms and local actors to discover opportunities organically. Policy should act as a gardener, not an architect."

Oliver Schoppe, UVC Partners

Selected Players

EWOR · Nucleate · UNTERNEHMERTUM · RISE EUROPE · KTH VETENSKAP OCH KONST · STATION F · GovTech Campus Deutschland · eXIST Existenzgründungen aus der Wissenschaft · université PARIS-SACLAY · The MBA Fund



RETAINING TALENT BY ENABLING MOBILITY

Streamlining Cross-Border Relocation to Retain and Attract Skilled Talent

Europe's capacity to attract skilled talent is consistently weakened by its inability to manage the practicalities of relocation [421]. The complex logistics of moving, such as visas, housing, and family integration, often outweigh the professional benefits of a new position [422]. This friction creates a significant leak in Europe's talent pipeline, wasting recruitment resources and reducing competitiveness [423].

The central opportunity is not another job portal, but a focused effort to address the obstacles between a job offer and successful settlement. This requires moving beyond digital tools that only match candidates with vacancies, toward integrated systems that actively facilitate the relocation process [424].

A range of solutions can emerge in this space, from simplified digital procedures that consolidate bureaucratic tasks to support services that assist with housing, child care, and partner employment. By redesigning the relocation experience, Europe can turn a fragmented and tedious process into a smooth and reliable one. Reducing friction in cross-border movement would turn a major barrier into a clear advantage, directly enhancing Europe's ability to secure the skilled workforce its key industries require.

> "Companies highlight talent shortages and bureaucracy as key hurdles. Europe's stability and welfare attract talent, but these advantages fade when weighed against the stronger pull of global tech rivals."
>
> Alina Kontareva, Alexander von Humboldt Institute

Selected Players

andela · Avature · degreed · expatrio · iMocha · localyze · sirva · Toptal · VanHack · remofirst

SHARED DIGITAL COMMONS

INFLUENCING THE FUTURE OF DIGITAL SOVEREIGNTY

Unified Standards and Interoperability
Open Talent and Knowledge Sharing
Unified Digital Payment Infrastructure

Cern in Geneva, Switzerland

Adil Köken 
Amelie Pöhnitzsch 
Edwin Daniel 
Estelle Kulow 
Jinjun Dong 

SHARED DIGITAL COMMONS

Common Foundations for European Resilience in a Digital Age

Shared digital commons refer to digital resources, such as data, software, and infrastructure, that are open and accessible to all. They function as public goods in the digital realm, much like roads or libraries do in the physical world. By framing payments, standards, and knowledge as shared infrastructures rather than private assets, digital commons extend the principle of public goods into the core of Europe's digital economy. When Europe pools resources, everyone benefits. Shared platforms lower costs, speed up crisis response, and build trust through transparent, democratic governance [425].

Digital commons offer not just tools, but new modes of governance that prioritize democratic decision-making over unilateral corporate control. The EU increasingly views digital commons as foundational to both innovation and sovereignty [426]. These commons combine open-source development, collective ownership, and decentralized governance models that protect against shifts in political or financial control [425]. They serve as democratic alternatives to proprietary systems, enhancing transparency and societal value beyond the simple sharing of resources [427]. Governance models that prioritize collective participation over profit-driven control are essential for creating equitable digital commons, which support broad access [428]. They also promote long-term resilience by reducing lock-in effects and enabling public institutions, SMEs, and researchers to remain independent of foreign technology providers. The EU is already implementing this. As the European Open Science Cloud enables scientists across member states to share research data under common standards, thereby breaking down silos and accelerating innovation [429]. NGI Commons is an EU initiative that creates a unified ecosystem of open-source software, hardware, and digital tools [430]. In finance, the Wero wallet unites 16 major banks to offer a European alternative to Visa and Mastercard [431].

However, building digital commons presents real challenges, especially when data sharing is involved [432]. Different national rules, competing standards bodies, and closed proprietary systems create fragmentation [432]. Publicly funded software should be open source, encouraging governments to support digital commons that serve the public good [433].

Three critical opportunities for strengthening digital commons have been identified. Establishing unified standards that ensure interoperability across systems reduce fragmentation and allow seamless collaboration across borders [434]. By creating open talent sharing and a skills-based collaboration platform, Europe's persistent skills gap can be bridged [440]. The third is the development of a unified EU payments infrastructure, treating financial rails as a digital commons to lower costs and reduce dependence on non-European providers [445]. With the right regulation, funding, and cooperation, shared digital commons can become the backbone of a sovereign, resilient digital Europe.

UNIFIED STANDARDS AND INTEROPERABILITY

Driving Standards to Enhance Interoperability and Secure Collaboration

Fragmented regulations, competing standards, and national silos undermine Europe's digital sovereignty [434]. They slow down seamless data sharing, complicate technical integration, and hinder efficient cross-border collaboration [435]. Without unified, open standards, SMEs and large enterprises face rising complexity and costs, while becoming more dependent on non-European technologies. This poses a threat to both competitiveness and long-term resilience [434].

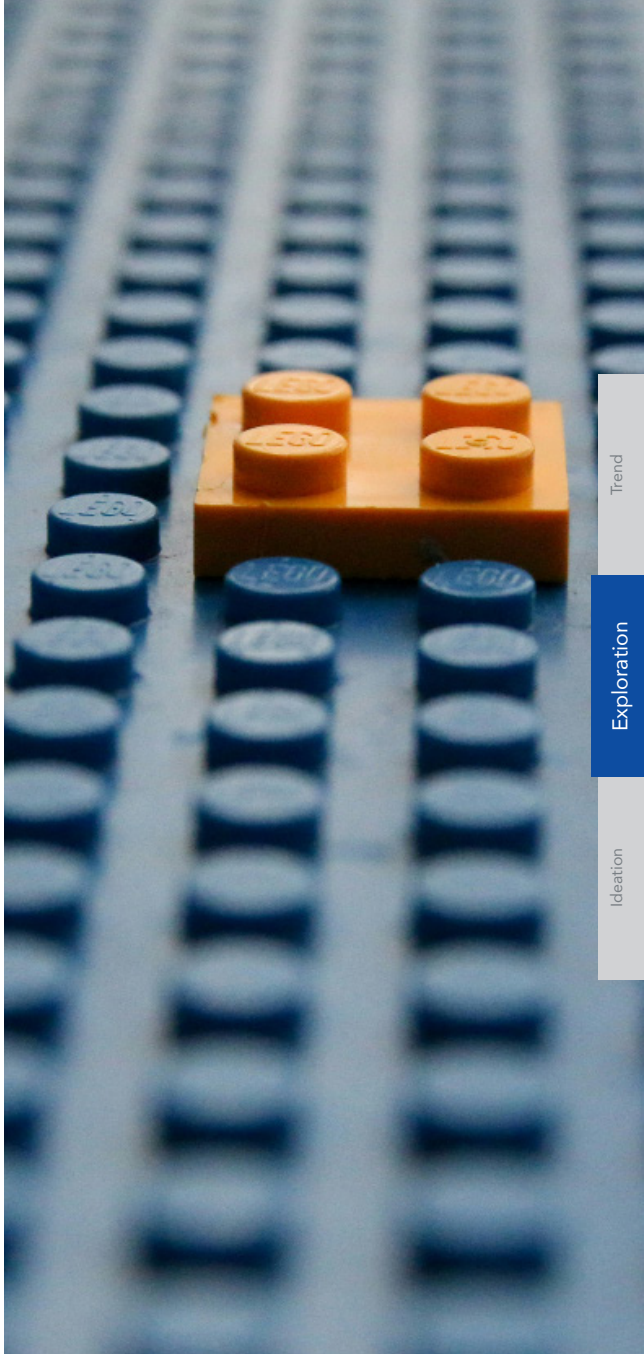
Europe urgently needs trusted, transparent interoperability layers that encompass open protocols, shared data formats, and federated governance to transform the digital commons from aspiration into reality. Initiatives such as Gaia-X demonstrate the promise and challenge of building a European-native infrastructure for secure and compliant data spaces. However, scaling these efforts requires better alignment and enforcement at the EU level. Integrating hardware-software architectures inspired by replicable, modular models can further accelerate convergence and innovation [436, 437].

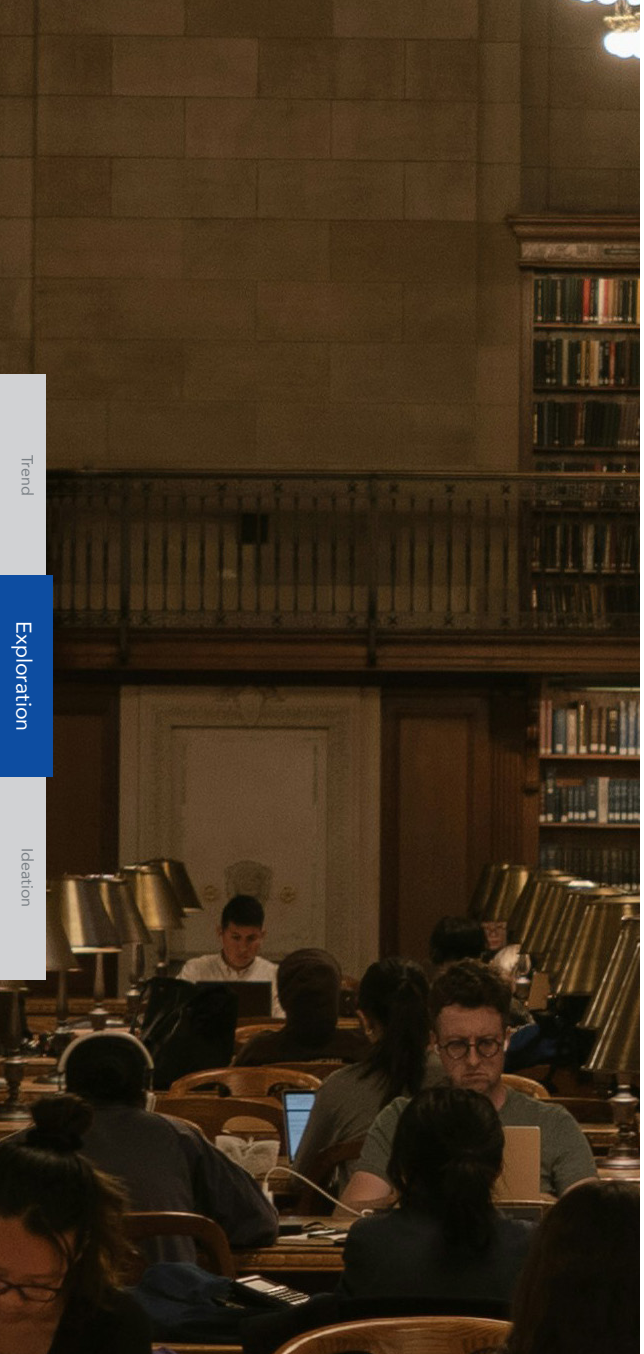
Investing in unified standards enables Europe to strengthen sovereignty, reduce fragmentation, and compete globally with agile, composable platforms and services. This is not just a technical challenge, but a strategic imperative to future-proof Europe's democracy, economy, and values in a multipolar digital world [434].

> "Europe should enforce digital regulations that mandate free and open-source technology, data sovereignty, and privacy."
>
> Prof. Francesca Bria, UCL [438]

Selected Players

Atos · T · ERICSSON · gaia-x · INTERNATIONAL DATA SPACES ASSOCIATION · Infineon · OWKIN · SIEMENS · IRIS² · EuroHPC Joint Undertaking





OPEN TALENT AND KNOWLEDGE SHARING

Connecting Talent and Skills to Demand via Cross-Company Collaboration

Highly specialized skills are becoming increasingly important for companies to stay competitive [439]. Since these capabilities are rarely in-house and evolve rapidly, finding the right people in a timely manner is challenging [440]. The most significant gaps lie in advanced IT, programming, data analysis, and mathematical skills [441]. Approximately 40% of executives report a shortage of workers capable of working alongside new technologies [441]. This gap is more pronounced in Europe than in the US, with 6 percentage points higher shortages in technological skills and 2 percentage points higher shortages in higher cognitive skills. As a result, firms depend on two sources: external knowledge and talent.

Open talent sharing offers a promising way forward. It is a skills-based model where companies can find, verify, and bring in external experts or teams on demand, either for short tasks like interviews or for embedded roles [440]. Platforms should match demand with supply, allocate work by skills.

AI can power this shift. By embedding it into recruiting systems, AI can actively scan the market, translate requirements into skills, and quickly surface strong matches, making a skills-first approach viable [442, 443]. However, organizations must protect data privacy and clearly govern IP, ensuring collaboration accelerates delivery without compromising control.

> “In the world of AI, knowledge is detached from talent, revolutionizing how we allocate work, build capabilities, and scale organizations.”
>
> Oliver Schoppe, UVC Partners

Selected Players

UNIFIED DIGITAL PAYMENT INFRASTRUCTURE

Building Sovereign, Seamless, and Secure Payment Rails for Europe

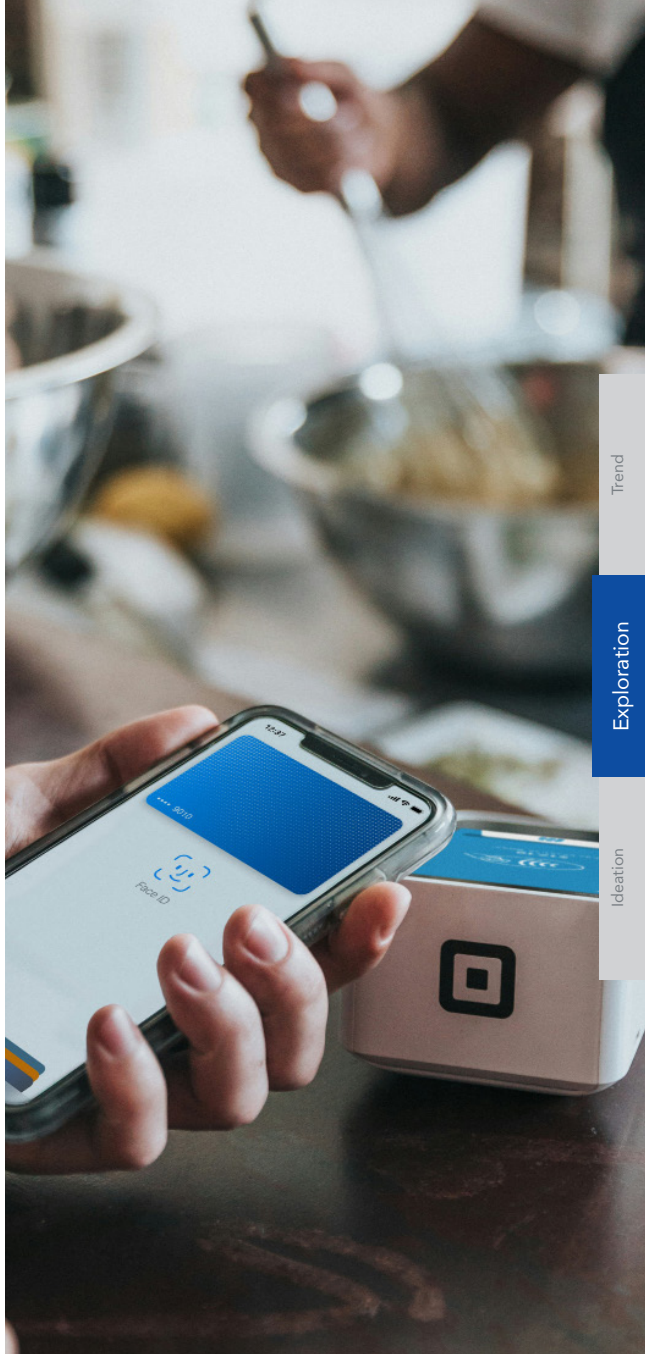
Europe's digital payments landscape consists of fragmented national schemes and a heavy dependence on foreign payment rails, including Visa, Mastercard, PayPal, and Big Tech wallets [444]. This reliance raises costs for businesses and consumers, limits interoperability, adds complexity to cross-border payments, and creates vulnerabilities in cybersecurity and sovereignty [445]. The absence of a unified framework undermines the EU's ability to build a fully integrated digital economy and weakens its strategic autonomy in critical financial infrastructure [445].

A Unified Digital Payment System offers the opportunity to consolidate diverse payment methods, such as bank transfers and cards, into a single, secure, and EU-governed framework. In the future, emerging means of payment like stablecoins and the digital euro can also be considered [446]. By treating payments as a digital commons, Europe can enable seamless cross-border transactions and reduce costs by about 510B USD [447]. This would also create trusted rails for public services like welfare and procurement, as well as for private innovation in fintech and embedded finance [448]. Such a system could become the foundation of Europe's digital sovereignty. It would improve efficiency, transparency, and competitiveness, while also promoting European standards of privacy, trust, and security in the global digital economy [448].

> "The digital euro project is a crucial step towards enhancing Europe's payments landscape and safeguarding our monetary sovereignty."
>
> Piero Cipollone, ECB [449]

Selected Players

adyen · Deutsche Bundesbank Eurosystem · Ledger · WERO · Klarna · Solaris · Trustly · Giesecke+Devrient Creating Confidence · Worldline



IDEATION

The following chapter describes five novel ideas of great relevance for *The Future of Digital Sovereignty*, especially in view of the identified future trends. Each of the ideas is developed to solve a specific problem in the identified problem spaces.

Adrian Stoica 
Andriani Nikolaou 
Charlotte Schöllkopf 
Gjergj Kukaj 
Karolina Wick 
Malte Oberhoff 

CORAL

Privacy Where It Matters, Compute Where You Need It

CORAL (Computational Resource Allocator) is a software platform designed to address the growing complexity of hybrid computing environments. Modern organizations now integrate on-premises servers, edge devices, and cloud services, but this combination raises challenges with cost, latency, and data protection [450]. The growing use of large language models (LLMs) increases the need to assess data sensitivity before processing, as employees depend on these tools for handling sensitive or confidential data [451]. Additionally, the rise of real-time applications heightens the need for reliable edge computing, making efficient resource allocation and coordination across distributed infrastructures crucial [21, 450].

CORAL solves these challenges by delivering intelligent, secure, and cost-effective orchestration for modern computing environments. It automatically determines where each computational task should be processed by evaluating latency, computational effort, expected cost, and data sensitivity and privacy requirements. CORAL can use existing metadata, such as document classification or device context and analyze requests to support real-time decisions.

For example, factory robots or retail checkout cameras can be prioritized for local execution to meet strict latency needs, while sensitive data like intellectual property or customer information remains on-premises for compliance and privacy. Less sensitive or more compute-intensive tasks are shifted to the cloud when efficient. This dynamic allocation reduces reliance on hyperscalers for sensitive data and lowers egress and bandwidth costs, which have become significant in cloud-based AI workloads.

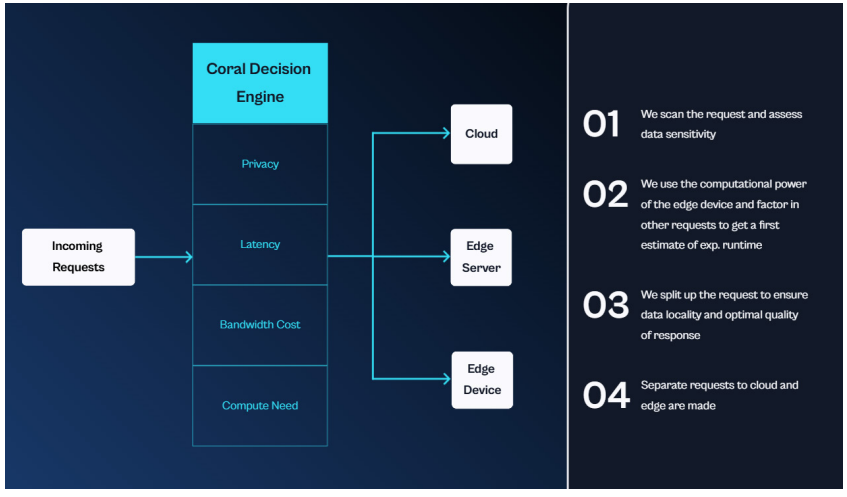
By combining privacy protection, efficient resource use, and better service quality, CORAL allows companies to manage workloads without deep infrastructure expertise. This is especially important for SMEs lacking in-house specialists or facing high upfront server investment costs. Manufacturers, retailers, and businesses managing sensitive data can set policies, monitor tasks, and optimize spending from a single interface.

While most competing solutions focus on technical efficiency, CORAL stands out with its privacy-first approach that balances compliance, performance, and resource control, supporting greater digital autonomy for users.

Problem

- Static load balancing and resource allocation in hybrid cloud architecture hinder efficient workload distribution, creating significant allocation challenges and reducing overall system performance [450, 452].
- Without task offloading strategies in edge computing, compute-intensive and delay-sensitive applications face excessive latency, high energy consumption, and reduced security, which limits scalability and real-time responsiveness [453].
- Deploying LLMs in sensitive domains such as healthcare, finance, and legal services risks exposing private data and compromising security, making robust sensitivity detection mechanisms essential [451].
- Multi-cloud tools without provider-agnostic orchestration rely on specific providers and manual configuration, leaving workloads vulnerable to failures, adding operational complexity, and making reliable management across environments difficult [454].

Enterprises face rising costs, compliance risks, and performance bottlenecks because hybrid cloud systems lack dynamic workload orchestration.



Solution

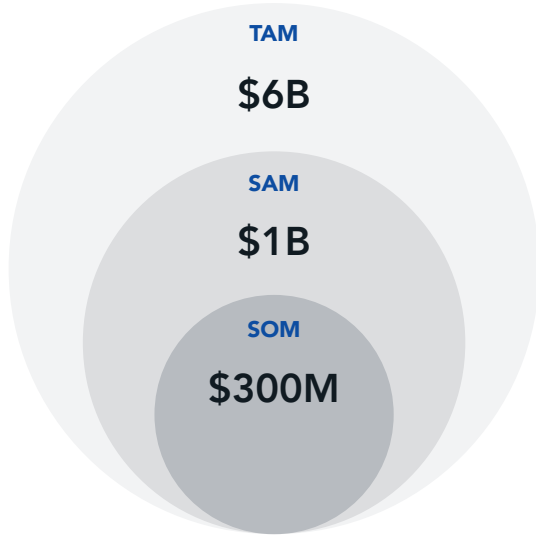
- CORAL acts as a decision engine between incoming requests and compute resources, assigning which part of each task should run locally or in the cloud.
- It evaluates various factors such as latency, data sensitivity, current server load, payload size, bandwidth capacity, and cost, using existing metadata and contextual information to guide decisions. When metadata or context is missing or insufficient, CORAL can use AI models trained for real-time request analysis to suggest where to execute tasks.
- By requesting splits continuously, high-priority or sensitive parts remain local, while less sensitive or compute-intensive parts are offloaded to the cloud. This balances the load and ensures information is processed in the most efficient way possible.
- The tool prefers local execution to minimize transfer energy, apply admin-defined rules, such as jurisdiction, cost, and service level agreements, and provide metrics for utilization, latency, and cost.

CORAL routes each request to the right location, ensuring compliance with data residency requirements while reducing costs.

Market

- In the EU, more than 53,000 large enterprises (with 249 or more employees) exist. It is expected that a large share of the enterprises form the core buyer segment for hybrid cloud orchestration [455].
- Worldwide edge investments are projected to reach 378B USD by 2028, up from an estimated 261B USD in 2025, showing sustained double-digit growth and expanding budgets for orchestration [456].
- The global hybrid cloud market is valued at approximately 173B USD in 2025 and is forecast to nearly double to 312B USD by 2030, growing at a CAGR of 13% [457].
- Besides hybrid cloud setups, 89% of enterprises report multi-cloud usage, reflecting the growing reliance on diverse cloud providers to optimize flexibility and cost efficiency [458].
- When selecting workload venues for AI, 42% of companies surveyed in 2025 consider latency and proximity requirements, while 11% of enterprises allocate their AI workload at on-premises infrastructure [459].

Enterprises are rapidly adopting multi-cloud and edge computing, with EU regulations and large firms driving demand for secure orchestration.



Competition

- Existing solutions have focused mainly on privacy and security in cloud computing and cloud-native contexts, for instance, by decentralizing cloud computing, such as Akash [460].
- Solutions centered around hybrid clouds and edge device integration with on-premise data centers are focusing heavily on the orchestration of computations across the infrastructure.
- Orchestration platforms like ZEDEDA or RAFAY, integrate into existing edge architectures and optimize for factors such as computational complexity, resource needs, and latency requirements [461, 462].
- CORAL adds personalized privacy as a parameter to the orchestration engine, keeping requests dynamically secure and giving customers full control over privacy needs and computation location. It is a sovereign-first solution, closing the gap between privacy and performance in existing market solutions.

CORAL is a dynamic orchestration tool that allocates workloads based on performance, efficiency, and data-sensitivity aspects.

Assumption Tree

Resource Allocation is a Challenge

Hybrid and multi-cloud setups are widespread. Yet, orchestrating them adds significant complexity in regards to resource allocation. SMEs and enterprises lack expertise or tools to decide where workloads should run. This leads to wasted resources, higher security risks, and inefficiencies that slow down their business.

Privacy & Compliance Drives IT Purchasing

SMEs and enterprises in regulated industries, such as finance, healthcare, and manufacturing, need to ensure that sensitive data remains on on-premise servers or on the edge. Compliance requirements, such as GDPR, create a demand for orchestration tools that optimize for data locality, security and privacy.

Cloud Bills are Challenging

Cloud bills can be unpredictable and often higher as expected. SMEs and enterprises are actively seeking ways to balance cloud, on-premises, and edge workloads to reduce costs without compromising performance. This creates a market demand for orchestration tools that optimize for costs and load balancing.

Need for Vendor-Agnostic Orchestration

Existing solutions like AWS Outposts, Azure Arc and Google Kubernetes Engine are powerful, but lock customers into a single ecosystem. Therefore, many companies prefer flexible, vendor-agnostic platforms that allow freedom of choice in regards to the cloud-architecture while offering easy deployment and monitoring.

Demand for Privacy-First Orchestration

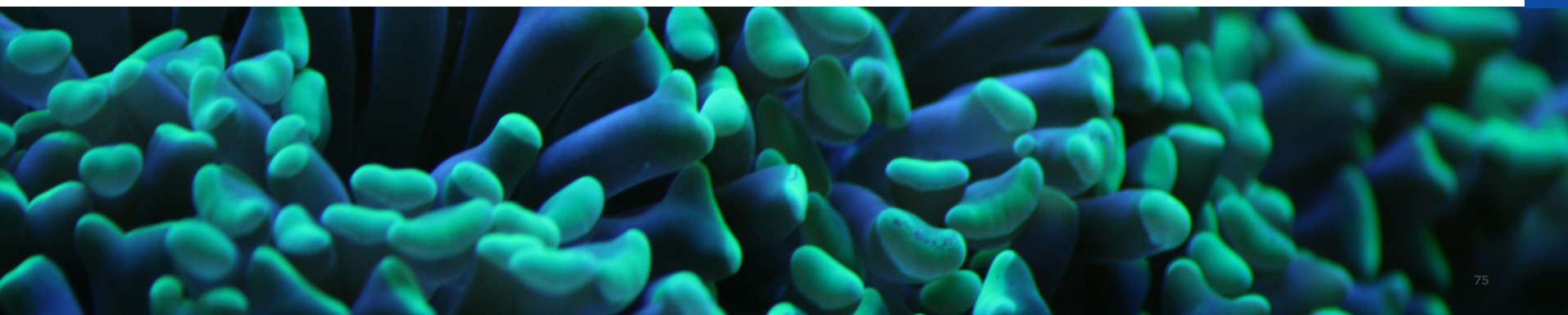
The growing complexity of infrastructure, combined with strict compliance requirements, is pushing organizations to adopt platforms that simplify hybrid cloud orchestration while keeping sensitive data local. With LLMs becoming part of everyday business, the demand for privacy-aware orchestration grows.

Demand for Cost-Efficient Orchestration

High costs and vendor lock-in leave enterprises looking for alternatives. A neutral, lightweight platform that integrates across providers while reducing cloud spend would address a pressing market problem. An orchestration layer that includes on-premises and edge resources differentiates itself from competitors.

Demand for Multi-Parameter Orchestration

Given the demand for privacy-first orchestration and cost-efficient, vendor-neutral platforms, a clear demand exists for a multi-parameter orchestration tool. Such a tool can position itself as a trusted, central platform that empowers SMEs and enterprises to balance privacy, performance, and cost.



Anjella Klaiber 
Hanano Shiga 
Jakob Limmer 
Jonathan Mäusle 
Katy Grossman 

materiOS

Building the Backbone of AI-Enabled Material Discovery

Europe's technological sovereignty is increasingly shaped by the global dynamics of critical raw materials (CRMs) [463]. As the shift toward greener and more digital economies accelerates, the need for rare earth materials continues to rise [463]. Yet securing these resources is no longer just a matter of physical supply chains. Advances in science and technology now rely heavily on the generation, integration, and protection of complex research data [464]. Within this research area, fragmented infrastructures and the reliance on non-European platforms slow down discovery and commercialization, while also exposing Europe to risks around strategic autonomy [465].

At the same time, the materials research landscape remains fragmented, with tools and techniques for computational modeling, data management, and ML often developed independently, creating isolated silos that hinder interoperability [466]. Researchers frequently need to manually combine outputs from these tools, resulting in duplicated effort, poor reproducibility, and delays in discovery. Current approaches to overcome these issues that rely on either generic enterprise software or custom-built pipelines are expensive, difficult to scale, and lack robustness [467].

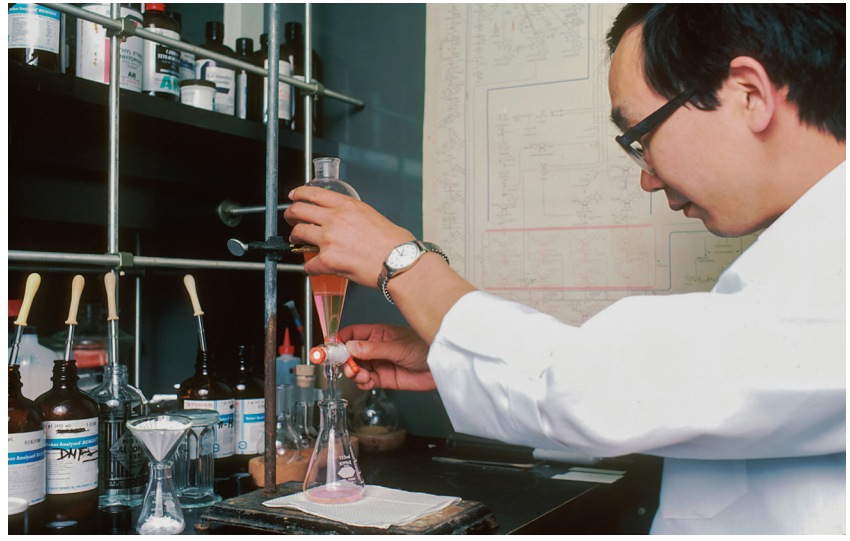
This scattered infrastructure presents a significant barrier to advancing materials innovation. Unlocking progress requires unified systems that allow data to flow efficiently across different tools. Such integration shortens development timelines, improves reproducibility, and fosters collaboration. Without it, valuable data remains underutilized, insights are delayed, and the pace of discovery falls short of meeting urgent technological, environmental, and geopolitical challenges [467, 468].

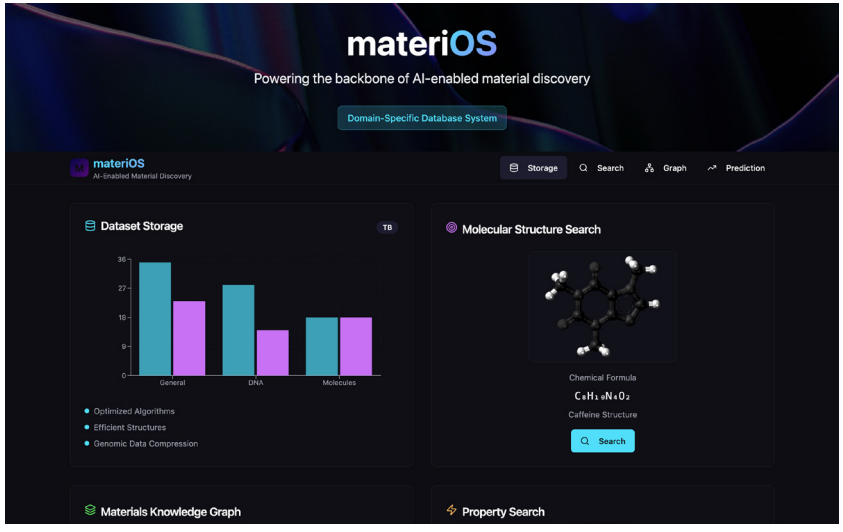
The fragmentation of materials data is both a challenge for fast material discovery, but also a chance to build solutions that unlock its full potential. materiOS proposes a solution by providing a domain-optimized data Operating System (OS) designed for heterogeneous material data. It combines material-specific data indexing and compression with application-specific query processing to support machine learning, visualization, reporting, and collaborative workflows. By standardizing data formats and metadata while preserving data sovereignty, materiOS turns disconnected datasets into actionable insights, accelerates time-to-discovery, and enables secure, cross-institution collaboration, allowing researchers to focus on discovery rather than infrastructure.

Problem

- The end-to-end process for discovering, developing, and commercializing a new material typically takes up to 20 years, a timeline that is incompatible with today's rapid technological, environmental, and geopolitical challenges [469].
- The European Union currently imports around 98% of its critical rare earth elements from China, highlighting both the urgency of developing local solutions and the vulnerability created by supply chain concentration [470].
- Material discovery is hindered by fragmented and heterogeneous datasets, which slow down efficient analysis and limit knowledge generation [468].
- Current materials science infrastructures often lack standardized, integrated workflows and long-term maintenance support, leading to fragmented tools and platforms that can be difficult to scale, integrate, and sustain [468].

Material discovery and commercialization face slow timelines, supply chain risks, fragmented data, and poorly integrated infrastructures.





Solution

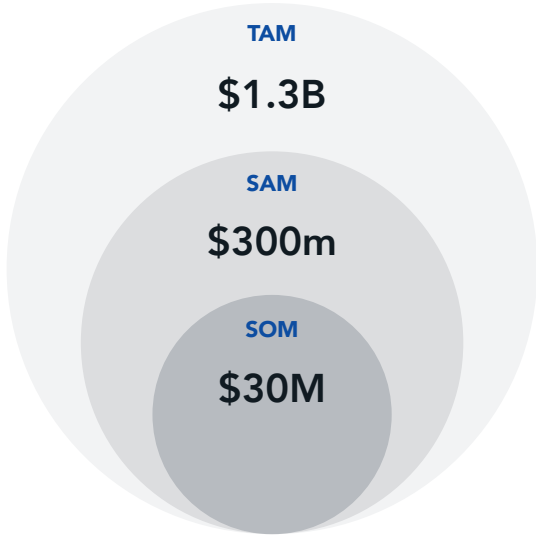
- materiOS is a unified, domain-optimized data infrastructure designed to manage the rapidly growing volume and complexity of material discovery data.
- It ingests, stores, and indexes diverse data types, including material properties, molecular structures, and simulation trajectories, while applying domain-specific compression and indexing to reduce storage costs and deliver fast, scalable querying.
- The platform brings together AI, collaboration, and reporting tools to turn raw data into actionable insights, significantly shortening discovery cycles.
- By standardizing data formats, materiOS enables reproducibility, seamless collaboration across institutions, and the creation of sovereign, interoperable material data ecosystems.
- Its secure and federated access model allows stakeholders to collaborate and share results without centralizing sensitive or IP-critical data, ensuring that control remains with data owners.

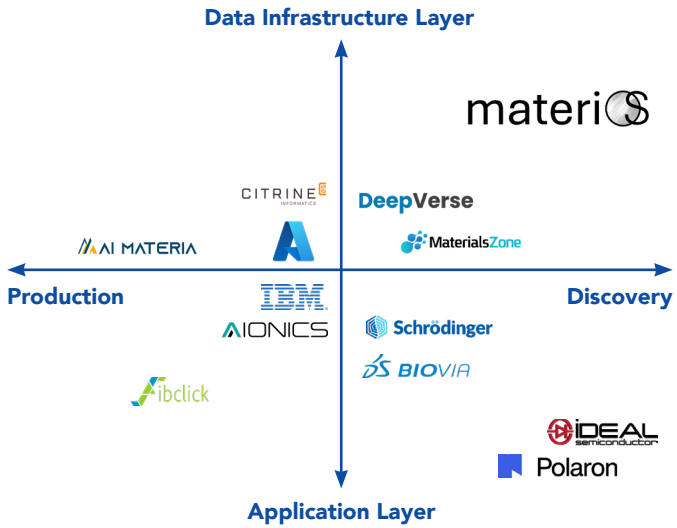
materiOS enables researchers to unify and harness their data, accelerate every stage of discovery, and take full control of the future of materials.

Market

- The market potential for materiOS can be observed both within Material Informatics and more broadly across AI-driven material discovery platforms.
- The global market for AI-driven material discovery platforms is valued at approximately 1.3B USD and projected to grow to nearly 12.5B USD by 2034 [471].
- Europe represents roughly 300M USD of the total market, supported by substantial research funding, government initiatives, and industrial adoption. It serves as a strategic base for expansion into North America and the Asia-Pacific [472, 473].
- Capturing a 10% share of the European market could generate 30M USD in near-term revenue.
- Industry forecasts indicate 18–25% annual market growth between 2024 and 2030, fueled by the integration of artificial intelligence and machine learning combined with the push for sustainable materials and cost-efficient innovation [471, 472].

materiOS taps into Europe's growing material discovery market and leverages its capabilities to drive global growth.





Competition

- Established enterprise software firms, such as Dassault Systèmes and Schrödinger, offer comprehensive platforms. Their strength lies in their extensive user base and deep integration with other enterprise tools, yet they often lack the domain-specific optimization necessary for cutting-edge materials research [473].
- Specialized material informatics startups, such as Citrine Informatics and MaterialsZone, provide advanced, purpose-built, AI-driven solutions exclusively for the materials science domain. They excel in the application layer, but they are built on general-purpose database systems without domain-specific advancements [472].
- General-purpose data and AI platforms from major tech companies like IBM and Microsoft offer powerful, generic tools that can be customized, but they lack built-in domain expertise, curated data models, and specialized workflows [474].

materiOS transforms material discovery with a unified data management system combining efficient storage with seamless collaboration.

Assumption Tree

Growth in Data Volume

As material discovery becomes more data-driven, the accelerating growth of research data will soon exceed the capacity of existing infrastructures. Without scalable and efficient systems for managing, integrating, and analyzing this data, discovery cycles will slow, reproducibility will suffer, and Europe's ability to compete will be constrained.

Data Model Mismatch

Traditional relational databases are not optimised for processing material discovery data, such as molecular graphs, genomic sequences, and multi-dimensional simulation trajectories. Their rigid schemas and lack of native support for sequence- and graph-based data result in slow queries, costly processing, and poor scalability.

Fragmented Research Landscape

Significant progress has been made in genomic compression, graph databases, and AI-driven material discovery. However, these advances remain siloed across disciplines and tools. Without integration, researchers must manually stitch together workflows, limiting scalability, reproducibility, and efficient collaboration.

Lack of Unified Infrastructure

There is no unified, domain-specific platform that combines storage, compression, advanced querying, ML pipeline orchestration, and collaboration tools for material discovery. Researchers rely on fragmented, custom-built toolchains that are expensive to maintain, hard to scale, and unable to meet the data demands of material discovery.

Growing Data Management Bottlenecks

The exponential growth of material discovery data, combined with the limitations of relational databases, creates severe data management bottlenecks. Researchers face slower query times, excessive preprocessing, and scalability issues, which hinder the timely delivery of insights and delay the overall discovery process.

Fragmentation-Induced Inefficiency

Because there is no unified infrastructure for material discovery, data remains fragmented across incompatible formats and tools. This forces researchers to spend significant time on preprocessing and integration tasks, resulting in duplicated effort, higher storage and computational costs, eventually slowing down the adoption of AI-driven workflows.

Infrastructure for Material Discovery

The fragmentation of workflows and data sources is a key barrier to scaling data-driven material discovery. materiOS addresses this by unifying these functions in a single tailored platform. It demonstrates that integrated infrastructure can streamline data handling, accelerate discovery, and ensure sovereign control of research data.

Benedikt Albertsen

Danit Newattananan

Niklas Remiger

Nikolas Keller

Salan Isaqzoi


Skyrise

Skyrise

Protecting European Interests in Space

Strategic autonomy is inseparable from the reliable use and long-term protection of space [475]. Europe's critical infrastructure, including defense, communications, and navigation, relies on satellite networks that are indispensable but vulnerable [476]. The orbital environment in which these networks operate is increasingly hostile. Decades of space activity have left thousands of defunct satellites and rocket fragments circling Earth [477]. Some pieces are small but fast-moving, capable of disabling an active satellite with significant impact. Others are large, such as inactive satellites weighing several tons, which pose catastrophic collision risks if left uncontrolled.

Different methods exist to address orbital debris, all aiming to capture and slow down objects. Each approach faces technical challenges, from ensuring secure attachment to targets traveling at 28,000 km/h to avoiding further fragmentation. Despite years of research, large-scale and reliable debris removal has yet to be achieved. This unresolved issue leaves Europe's satellite fleets exposed to a growing and unpredictable danger.

At the same time, deliberate threats are multiplying. Anti-satellite weapons, developed by several major powers, demonstrate the ability to disable or destroy satellites through direct strikes or by creating large debris fields that threaten entire orbits [478]. These weapons are part of broader strategies of space denial, where one actor seeks to limit another's access to orbital services. For Europe, which depends on uninterrupted satellite connectivity for military coordination, civil security, and economic activity, this represents a direct strategic risk.

Skyrise is developing a dual-use orbital protection spacecraft designed for Europe. The system combines two functions in one device: autonomous interceptor satellites to capture and remove hazardous debris and the ability to respond to hostile actions in orbit. Unlike initiatives that separate debris removal from defense, Skyrise unifies them. This integrated capability reduces immediate collision risks while building the basis for credible long-term security applications. Skyrise enhances Europe's resilience in space by reducing reliance on external systems and ensuring the security of satellite networks.

Problem

- Since the launch of the first satellite in 1957, Earth's orbit has filled rapidly with over 15,000 active satellites and projections of nearly 70,000 by 2035, driven by falling costs and rising investment [479, 480].
- Satellites support vital infrastructure, including navigation, secure communications, disaster response, climate monitoring, and global connectivity, making space safety a key economic and security concern [481].
- In low-Earth orbit, the European Space Agency (ESA) estimates that the number of inactive satellites, rocket debris, and large fragments now exceeds the number of active satellites, further intensifying collision risk [482].
- Each collision can create thousands of high-velocity shards, driving cascading failures that could render orbits unusable for decades [483, 484].
- The removal of large, defunct satellites is essential to cut systemic risk, safeguard essential services, and preserve sustainable access to space [485].

Protecting orbital infrastructure requires Europe to combine cyber strength and space defenses before adversaries exploit gaps.

Solution

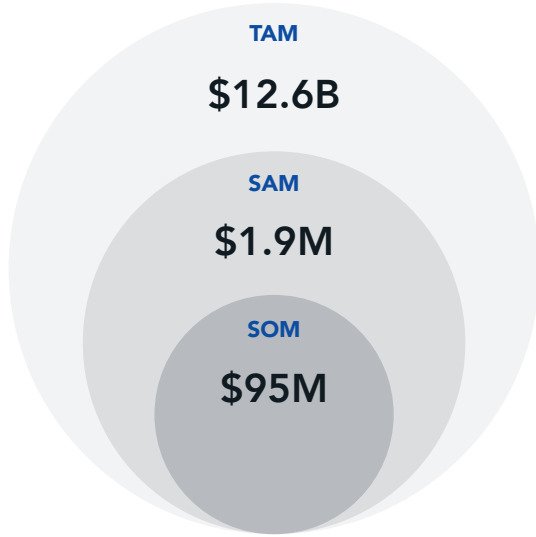
- Skyrise is building Europe's first orbital guardian spacecraft, deploying interceptor satellites to shield assets from debris and derelict objects.
- Satellites use precision propulsion and non-lethal techniques to protect infrastructure. Air launching enables rapid response and safe disposal in the graveyard.
- Starting with commercial operators, the platform tackles orbital congestion. Protecting constellations from collision risk ensures uninterrupted service and long-term sustainability.
- The solution strengthens European sovereignty by enabling satellite protection, reducing reliance on foreign systems, and securing future orbital resilience.
- Proven in commercial markets, the platform evolves toward dual-use applications, with government adoption extending protection from private constellations to defense applications.

Skyrise provides an autonomous device that shields satellites from debris and collisions, ensuring secure and sovereign access to space.

Market

- Over 15,000 active satellites now populate Earth's orbit, with projections indicating this number could reach nearly 70,000 by 2035 [479, 480].
- Global spending on space defense is rising sharply. In 2023 alone, the US invested approximately 38.9B USD, China 8.8B USD, and Russia 2.6B USD, directed toward manufacturing, secure communications, and space domain awareness [486].
- The EU is ramping up funding, with the European Defense Fund investing over 8B EUR since 2021, alongside new initiatives to mobilize funds in private finance for space defense innovation [487, 488].
- The US conducted its first successful anti-satellite (ASAT) test in 1959, demonstrating the feasibility of such weapons [489]. Today, expanding investments by e.g., the US, China, and Russia suggest that the risk of other nations targeting satellites is likely to increase [490].

Rising global and European investments are driving the emergence of a rapidly expanding market for space defense.



Debris Management

Competition

- Debris capture and deorbiting specialists, including Astroscale, ClearSpace, Turion Space, GMV, and Kall Morris, pioneer robotic arms, adhesion capture systems, and grappler-equipped satellites to actively capture, redirect, and safely deorbit space debris [491, 492, 493, 494, 495].
- Laser-based removal actors, such as Orbital Lasers, explore non-contact ablation to nudge or deorbit debris, with services planned by 2026 [496].
- Ground-based anti-satellite defense, such as Lockheed Martin, Northrop Grumman, and Raytheon, fields mature missile interceptors and directed-energy weapons that set today's defense benchmark [497].
- Space-based defense innovators, including Dark, GuardianSat, and Impulse+Anduril, develop air-launched interceptors, AI-driven counter-ASAT systems, and maneuverable satellites designed for rapid orbital response [498, 499, 500].

Bridging commercial debris removal and sovereign defense, our dual-use platform delivers a unique European solution for space protection.

Assumption Tree

Space Economy is Expanding Rapidly

The global space economy is growing, with satellites enabling essential services such as communication, navigation, and earth observation. Rising demand for access to orbit makes secure and reliable operations vital for both economic growth and strategic resilience.

Orbital Debris is a Mounting Risk

Decades of launches have filled orbit with inactive satellites, spent rocket stages, and fragments. Even small debris traveling at high velocity can disable active satellites. With no scalable removal methods, Europe's fleets remain exposed to escalating collision risks.

Europe Needs Sovereign Satellite Defense

Europe's dependence on external systems creates strategic vulnerabilities. Sovereign satellite capabilities are essential to reduce dependence on the US and ensure digital sovereignty. Secure and independent access to orbit is critical for defense and security.

Satellites Face Rising Hostile Threats

Anti-satellite weapons and electronic interference are turning space into a contested environment. Major powers have already demonstrated the ability to destroy or disable satellites, often by generating dangerous debris fields.

Satellite Growth Requires Debris Removal

Growing reliance on satellites cannot be sustained without reliable debris removal. Effective solutions reduce collision risks, extend lifetimes, and safeguard constellations. Without them, both economic activity and critical infrastructure are at risk.

Europe Must Actively Defend its Satellites

To safeguard sovereignty and security, Europe requires active protection of satellites against hostile actions. Defensive measures ensure uninterrupted navigation, communication, and military coordination, supporting resilience and autonomy.

Dual-Use Spacecraft Remove Debris and Defend

Europe needs spacecraft that can both remove hazardous debris and defend satellites against threats. Recognizing that these capabilities are operationally distinct but technologically identical, combining them in one platform reduces collision risks and counters hostile actions, securing infrastructure and autonomy in space.

Ammar Idriz 
Joe Lammers 
Joseph Gawlik 
Linnea Brand 
Tarak Amouri 

Cyberlingo

Making Cybersecurity Compliant, Personalized, and Fun

Across Europe, companies are facing a digital skills crisis. In 2023, 32% of Europeans lacked basic digital skills such as recognizing phishing attempts, judging the credibility of online information, and managing secure passwords [501]. Concurrently, regulatory pressure is on the rise: under the NIS2 directive, demonstrable cybersecurity compliance has been required since 2024 [501].

With the current trajectory, 60% of the EU population is predicted to possess at least basic digital skills by 2030, which falls short of the target of 80% [502]. For SMEs, this creates a double burden. They often lack the budgets and in-house expertise to provide training, yet they face the same compliance obligations and risks as large corporations.

Current corporate learning approaches, including lengthy workshops, generic video courses, or expensive providers, often fail to deliver. Research indicates that 80% of newly acquired knowledge is forgotten within just one month, leaving employees disengaged and companies vulnerable [503]. It also shows that customized cybersecurity awareness training programs significantly reduce security incidents in SMEs by addressing specific contextual factors and promoting practical application [504].

Cyberlingo addresses this urgent gap with a gamified learning app designed specifically for SMEs. The app begins with a baseline assessment of an employee's digital literacy and cybersecurity awareness, then builds a personalized learning path adapted to their role and skill level. Training is delivered through 5–10 minute weekly micro-lessons, reinforced with AI-driven spaced repetition to maximize retention. Employees are motivated by gamified elements, such as streaks, challenges, and leaderboards, which make learning an engaging and consistent experience.

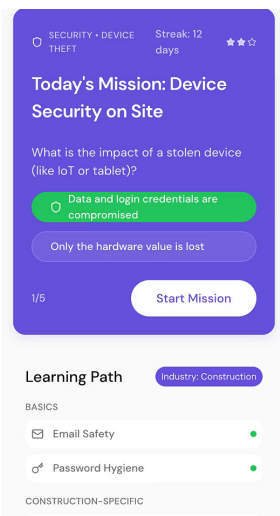
For managers, Cyberlingo provides a dashboard to anonymously track progress and compliance in real time, ensuring teams not only build skills but also generate auditable proof of NIS2 compliance. This combination of personalized content, gamification, and compliance tracking makes Cyberlingo uniquely effective in bridging the gap between regulation and workforce capabilities.

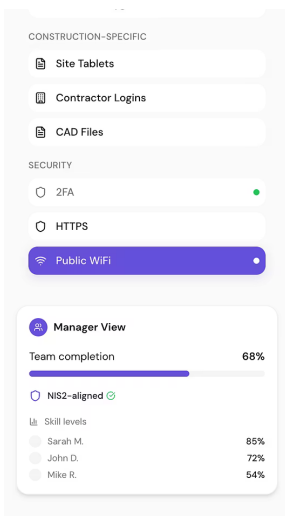
The market potential is significant. Europe's corporate learning and development market is valued at 40B EUR, growing at 17% annually [505], with cybersecurity training representing 930M EUR [506]. Unlike traditional providers, Cyberlingo delivers an affordable, scalable, and effective solution tailored to SMEs, transforming mandatory compliance into lasting digital resilience.

Problem

- Approximately 32% of Europeans lack the digital skills required in most jobs, highlighting a structural skills gap that risks limiting employability and economic competitiveness [501].
- The NIS2 directive mandates a high level of cybersecurity awareness for all staff. Non-compliance results in significant financial penalties and increases exposure to cyber threats [510].
- 74% of security breaches involve human errors, such as clicking on phishing links. Basic digital literacy and cybersecurity awareness can prevent many of these incidents [511].
- Traditional corporate training is often quickly forgotten, with 80% of the knowledge lost within a month. Slide decks and webinars rarely reflect daily work [509].
- In 2021, 23% of European SMEs offered digital skills training, compared to 70% of large firms. With fewer resources and a small IT staff, SMEs are particularly exposed to security risks [512].

A significant proportion of Europeans lack digital and cybersecurity skills, leaving SMEs, in particular, vulnerable to human errors and increasing cyber risks.





Solution

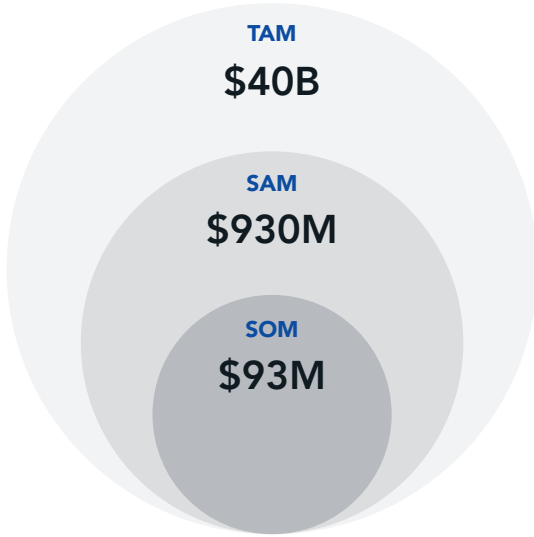
- Employees learn through 5- to 10-minute micro-lessons embedded in their daily tools, utilizing spaced repetition that has been proven to strengthen retention and align with modern attention spans [513].
- Gamified elements, such as streaks, XP, badges, and leaderboards, make training more engaging, increasing completion rates from 25% (without gamification) to more than 90% [514].
- AI-driven learning paths personalize content to each role, skill level, and company domain, allowing employees to focus only on skills that are relevant and impactful.
- Contextual real-time training delivers instant tips and challenges inside Outlook, Teams, or CRM, reinforcing secure behavior directly where work happens and reducing phishing failures.
- An integrated compliance dashboard assesses organizational skill levels, identifies gaps, measures ROI, and logs training records to meet NIS2 requirements while issuing certifications and badges.

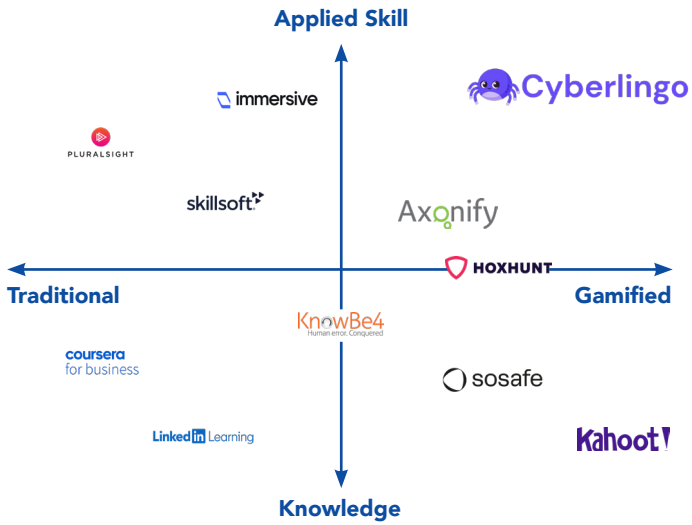
Cyberlingo makes cybersecurity training personalized and effective through micro-lessons, gamification, and real-time contextual learning.

Market

- Corporate learning and development is a ~40B EUR market in Europe, growing at 7.5% annually within a global industry exceeding 250B EUR. Yet, engagement and outcomes often remain low, leaving the sector vulnerable to disruption [515].
- Cybersecurity training is a 930M EUR market. Its growth comes from two main factors: the high and rising cost of human mistakes that lead to security breaches, and stronger rules that companies must follow [506].
- The EU's NIS2 Directive will require cybersecurity awareness programs for 160,000 companies, creating a regulatory push and accelerating adoption of scalable training solutions [516].
- SMEs remain underserved as they are in need of effective and personalized solutions that adapt to their operations and workforce needs [517].
- Capturing a 10% share of the European market would yield 93M EUR in annual revenue.

Cyberlingo taps into a 93M EUR opportunity in Europe's growing cybersecurity training market by addressing regulatory demand and underserved SME needs.





Competition

- Legacy training platforms, such as Pluralsight and Skillsoft, as well as corporate learning management systems (LMS), primarily rely on static course libraries and slide-based content [518, 519].
- General e-learning providers such as LinkedIn Learning, Udemy, and Coursera offer broad video libraries covering a wide range of professional skills, but their content is one-size-fits-all and rarely integrates with a company's internal tools and security systems, making it harder to deliver tailored and actionable training [516, 520, 521].
- Cybersecurity training apps, including KnowBe4, SoSafe, and Hoxhunt, typically focus on narrow use cases, such as phishing simulations and compliance [522, 523, 524].
- Consumer learning apps, such as Duolingo or Kahoot, demonstrate that gamification drives engagement, but primarily targets language or general knowledge, rather than digital literacy skills [525, 526].

Existing training solutions are often static, generic, or niche-focused, lacking integration, personalization, and scalable reinforcement to meet SME needs.

Assumption Tree

Compliance Pressure Creates Demand

EU regulations such as NIS2 make cybersecurity awareness and training mandatory [501]. SMEs must ensure employees have the required skills and provide auditable proof of compliance. Without visible action, they face financial penalties, reputational damage, and greater vulnerability to cyber threats in an increasingly regulated environment.

SMEs Are Vulnerable to Cyberattacks

SMEs are highly exposed to cyber risks, with human error responsible for up to 95% of breaches [507]. In the EU, 47% of SME owners feel unprepared for cyberattacks, while 67% admit they lack sufficient knowledge, and 48% do not even provide employees with training [507]. This creates urgent demand for cyber-training [508].

Context Drives Effective Learning

Current training is ineffective, with studies showing that 80% of knowledge is forgotten within one month [509]. Personalized lessons tied to daily tasks, workflows, and industry risks are far more effective, improving comprehension, retention, and the real-world application of digital and cybersecurity skills.

Micro-Learning Boost Retention

Short, adaptive lessons with gamified features such as streaks, challenges, and spaced repetition significantly improve engagement and retention. This approach ensures employees complete training, retain lessons over time, and actively apply digital and cybersecurity skills in their daily work, turning compliance into lasting digital resilience.

Urgent Compliance and Security Needs

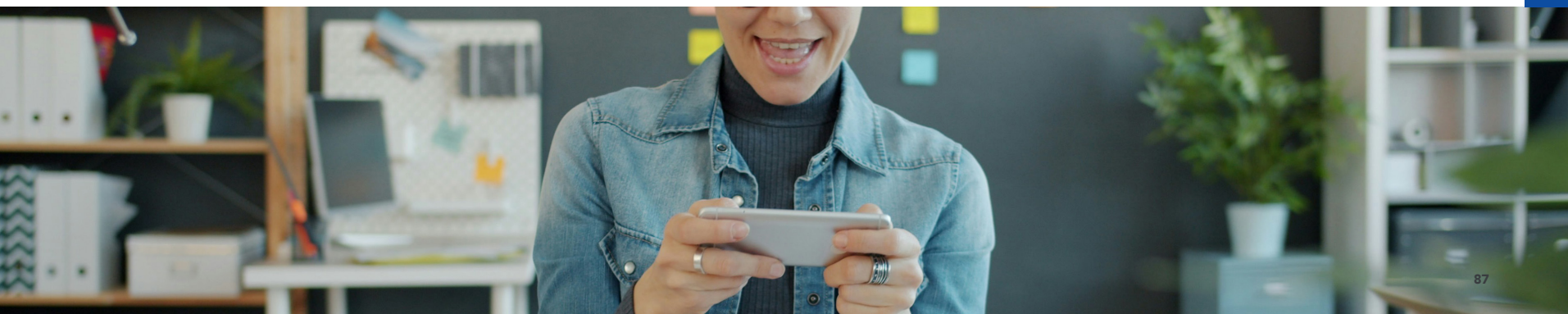
The overlap of strict regulatory obligations and disproportionately high cyberattack risks creates an urgent demand among SMEs for training solutions. These tools must be affordable and practical, closing skill gaps quickly while also providing auditable proof of compliance to regulators, insurers, and business partners.

Micro-Learning Beats Conventional Training

Corporate digital training is often ineffective, as generic programs are quickly forgotten and fail to develop lasting skills. In contrast, contextual, personalized, gamified micro-learning engages employees continuously, strengthens retention, and ensures that cybersecurity knowledge is applied in practice, protecting companies more effectively.

SMEs Require a New Training Approach

SMEs need a training solution that is affordable, personalized, and engaging, while also delivering auditable proof of compliance. Only approaches built on micro-learning, contextual relevance, gamification, and compliance tracking can close Europe's digital skills gap and meet the rising demands of regulation.



´Adil Köken 
Amelie Pöhnlitzsch 
Edwin Daniel 
Estelle Kulow 
Pedro Jinjun Dong 

SMartroutE

Frictionless Cross-Border Payments for SMEs

SMEs are the backbone of the European economy, with 26M firms representing 99% of all businesses and employing around 90M people [527]. Worldwide, they generate more than half of the global GDP [528]. Yet, despite their central role, SMEs face systemic hurdles in payments.

First, SMEs struggle to meet compliance requirements such as the Payment Card Industry Data Security Standard (PCI DSS), which increase costs and complexity. Securing financial transactions also demands dedicated IT infrastructure, including routing payments through separate network nodes rather than through the same devices used for other business operations. To cope with this, SMEs either need to invest in in-house knowledge, or rely on third party tools [529, 530].

Secondly, international payments often include hidden fees that are not transparent. Europeans and SMEs paid 30B EUR in 2023 alone in hidden fees [531]. Yet, SMEs increased their international sourcing by 61% compared to the previous year, despite difficulties with cross-border payments [532].

On top of these challenges, many SMEs remain locked into legacy systems and inefficient payment methods. Today's advanced solutions, from global payment service providers like Stripe and PayPal, primarily target large enterprises and digital-first companies. This leaves smaller enterprises underserved, facing transaction costs as high as 3% compared to less than 2% costs for large enterprises [533, 534].

SMartroutE addresses these challenges by acting as a smart payment routing engine tailored for SMEs. It simplifies security and compliance, removing the need for costly in-house expertise. By evaluating each payment across multiple payment service providers (PSP) in real time, SMartroutE optimizes for cost, speed, and reliability, and automatically handles cross-border regulatory requirements.

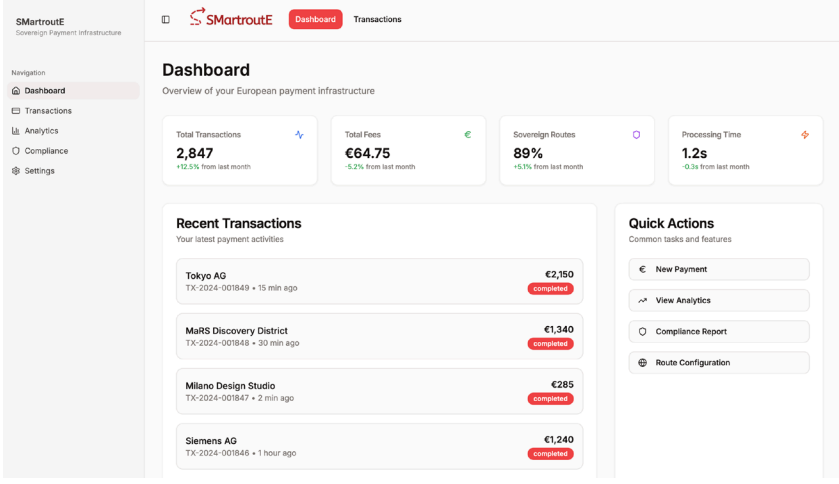
Its decision engine considers transaction size, destination, and urgency to determine the most efficient route, while also prioritizing European solutions. A user-friendly dashboard provides full visibility into payment flows, making hidden fees transparent and reducing them. Designed for non-technical users, SMartroutE requires minimal setup and no customer registration.

The tool seamlessly integrates new payment innovations, giving European SMEs enterprise-grade payment optimization without the complexity. The result is a provider-neutral, secure, and interoperable platform that adapts to SME needs, boosts financial resilience, and strengthens EU's strategic autonomy in digital finance.

Problem

- SMEs struggle with PCI DSS and other compliance requirements due to cost and complexity. They also struggle to manage financial transactions securely, as it requires dedicated IT infrastructure that is not shared with other devices [529, 530].
- International payment exchange rates are unclear, making it hard for SMEs to compare providers or costs. In 2023, these hidden fees cost European SMEs billions of euros [531].
- SMEs rely on PSPs to accept digital payments securely. Depending on a single PSP creates risks, including vendor lock-in with unfavorable pricing, a single point of failure and limited ability to optimize payment for costs or speed [536].
- Settlement delays of 2–7 days pose a serious challenge for SMEs. They tie up critical working capital, delay operations, and can lead to lost deals or revenue. SMEs lack financial buffers, making timely payments crucial for growth and business continuity [537].

Strengthen SMEs' cross-border B2B trade by cutting costs, speeding up settlement, and closing regulatory and information gaps.



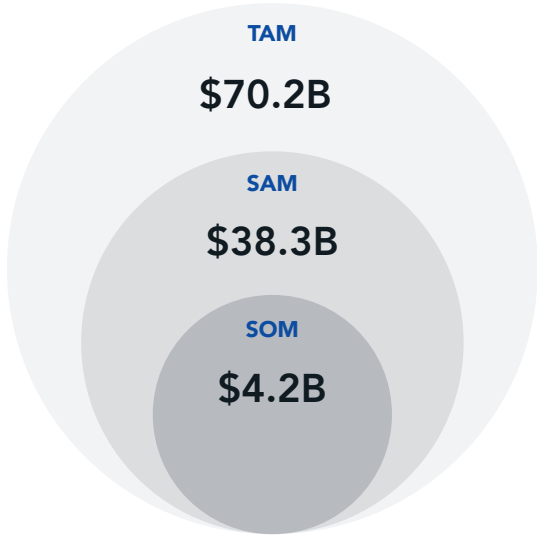
Solution

- SMartroutE is a payment routing engine that simplifies security and compliance, helping SMEs manage payments.
- The smart routing evaluates transactions across multiple PSPs, optimizing for cost, speed, and reliability while prioritizing EU-regulated infrastructure over foreign providers.
- The decision engine analyzes real-time factors such as transaction size, destination and urgency to determine the most efficient route, while also prioritizing European solutions where possible.
- Cross-border regulatory requirements are handled automatically, reducing complexity without dedicated legal resources.
- A dashboard provides full visibility into payment flows, showing each step, cost, and completion time while avoiding hidden fees.
- Designed for non-technical users, SMartroutE requires no receiver registration for customers, minimal setup, and automatically incorporates new payment innovations, making payment optimization accessible to all European SMEs.

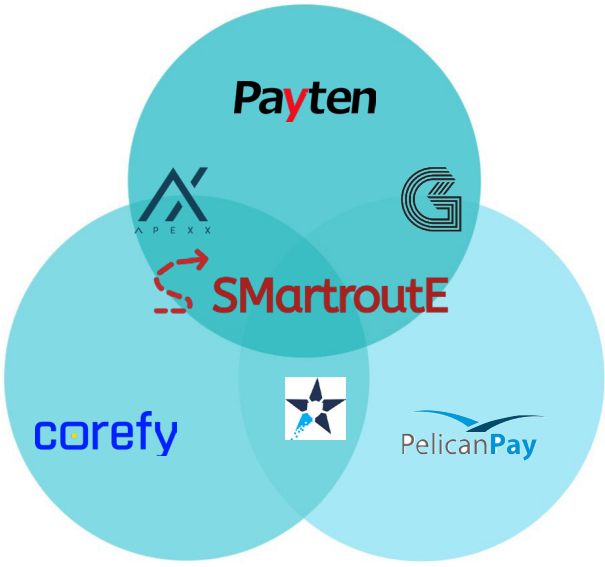
SMartroutE enables SMEs to cut costs, speed up settlement, gain transparency over fees, and stay compliant while prioritizing European solutions.

Market

- The European cross-border payments market is projected to generate approximately 64.4B USD in revenue by 2030, growing at a CAGR of 6.8% between 2025 and 2030 [538].
- SMEs increased their international sourcing by 61% compared to the previous year [532].
- Europe's real-time payments are estimated at about 7.21B USD in 2025 and projected to grow to 13.49B USD by 2030, at a 10.65% CAGR [539].
- Consumer-to-business flows held 53% of the European payments market size in 2024, with remittances and cross-border payments having the highest at 16.04% CAGR [540].
- The ECB highlights that Europe still lacks a unified pan-euro-area digital payment solution, leaving the euro area heavily dependent on foreign payment providers and reinforcing the need to build a sovereign and interoperable payment infrastructure [541].



SMartroutE targets a $64B cross-border payments market with an interoperable solution that limits reliance on foreign providers.



Competition

- Payten focuses on cost optimization through multi-bank POS switching and rule-based routing, but lacks advanced automation and machine learning capabilities for dynamic fee reduction [542].
- BR-DGE prioritizes payment speed and reliability by employing try-again mechanisms and cascading retries to minimize payment failures and improve approval rates [543].
- PelicanPay concentrates on compliance, offering automated payment flows, reconciliation, and adherence to European data privacy and security standards [544].
- Multifaceted providers like IXOPAY combine cost savings with enhanced payment success rates through multi-PSP connectivity and enterprise-grade routing [545].
- Gr4vy addresses compliance and risk management alongside cost or speed optimization, but does not provide full, real-time transaction-level transparency, limiting visibility into granular payment flows [546].

Competitors differ in their strengths, focusing either on compliance, transaction speed, or reliability. SMartroutE combines these strengths.

Assumption Tree

Legacy Systems Fail to Meet SME Needs

Most current payment infrastructures and solutions, such as those provided by Visa and PayPal, cater primarily to larger enterprises. As a result, SMEs remain reliant on inefficient legacy systems, characterized by high costs and limited transparency, excluding them from recent digital advancements.

Compliance Requirements Hold Back SMEs

Digital and international transactions require complying with regulations such as PCI DSS. This significantly increases both the complexity and cost of transactions for SMEs, as it requires certain IT-infrastructure and in-house knowledge. To cope with this, SMEs either need to build expensive in-house knowledge or rely on third-party-tools.

Hidden Fees Affect SMEs

In 2023 alone, European SMEs and consumers paid 30B EUR in hidden fees for cross-border payments [535]. SMEs are particularly vulnerable to these charges and unfavorable foreign exchange costs in international payments, which erode profitability and threaten long-term competitiveness, as smaller businesses typically have lower liquidity.

Persistent Payment Inefficiencies

Despite their important position in the European economy, SMEs continue to face systemic obstacles in payment processes, such as cross-border transaction delays and elevated fees. These inefficiencies contribute to significant financial strain, as many small companies face bankruptcy due to cash flow issues.

Need for Modern Solutions

SMEs face high costs and complexity from regulations like PCI DSS, while most payment infrastructures are built for large enterprises. Reliance on costly legacy systems limits access to modern payment capabilities, creating a clear need for streamlined, compliant, and efficient digital payment processes.

Overcoming Payment Inefficiencies

European SMEs face persistent payment inefficiencies, including cross-border delays and high fees. In 2023 alone, hidden charges and unfavorable exchange rates cost SMEs billions, eroding profitability and cash flow. These systemic obstacles limit competitiveness and financial resilience, making efficient, transparent payment processes critical.

Need for Efficient Payment Solutions

European SMEs are constrained by legacy systems, regulatory requirements, and payment inefficiencies, including hidden fees and payment delays. To remain competitive and protect cash flow, SMEs need compliant and transparent digital payment processes that simplify operations and reduce financial strain.

LIST OF CONTRIBUTORS

Adil Köken
Computer Science

Adrian Stoica
Philosophy

Amelie Pöhnitzsch
Business, Organizational & Applied Social Psychology

Ammar Idriz
Management & Technology

Andriani Nikolaou
Management & Digital Technologies

Anjella Klaiber
Management & Technology

Benedikt Albertsen
Business Administration

Charlotte Schöllkopf
Statistics & Data Science

Danit Niwattananan
Electrical Engineering & Information Technology

Edwin Daniel
Politics & Technology

Estelle Kulow
AI in Society

Gjergj Kukaj
Human Computer Interaction

Hanano Shiga
Consumer Science

Jakob Limmer
Software Engineering

Jinjun Dong
Robotics, Cognition, Intelligence

Joe Lammers
Management & Technology

Jonathan Mäusle
Sustainable Management & Technology

Joseph Gawlik
Data Science

Karolina Wick
Sustainable Resource Management

Katy Grossmann
Architecture & Civil Engineering

Linnea Brand
Resource Efficient & Sustainable Building

Malte Oberhoff
Management & Technology

Niklas Remiger
Mechatronics, Robotics & Biomechanical Engineering

Nikolas Keller
Business Administration

Salan Isaqzoi
Management & Technology

Tarak Amouri
Finance & Information Management

CDTM MANAGEMENT TEAM

Amelie Pahl
M.A. Management

Charlotte Kobiella
M.Sc. Management and Technology

David Meyer
M.Sc. Computer Science

Felix Dörpmund
M.Sc. Information Systems

Julia Balowski
M.Sc. Neuro Engineering

Martin Wessel
M.Sc. Data Science

Nikolaus Fischer
M.Sc. Psychology

Raunaq Jain
M.Sc. Sustainable Management
& Technology

Samuel Valenzuela
M.Sc. Computer Science

Vera Eger
M.Sc. Psychology

BOARD OF DIRECTORS

Prof. Dr. Albrecht Schmidt
Chair for Human-Centered Ubiquitous Media
Ludwigs Maximilians University

Prof. Dr. Alexander Pretschner
Chair of Software Engineering
Technical University of Munich

Prof. Dr. Andreas Butz
Chair for Media Informatics
Ludwigs Maximilians University

Prof. Dr. Dres h.c. Arnold Picot †
Chair for Information, Organization and Management
Ludwigs Maximilians University

Prof. Dr. Bernd Brügge
Chair for Applied Software Engineering
Technical University of Munich

Prof. Dr. Dieter Kranzlmüller
Chair for Communication Systems and Systems Programming, Ludwigs Maximilians University, Munich Network Management Team, Leibniz Supercomputing Center

Prof. Dr. Dietmar Harhoff
Director at the Max Planck Institute for Innovation and Competition

Prof. Dr. Hana Milanov
Entrepreneurship Research Institute
Technical University of Munich

Prof. Dr. Heinz-Gerd Hegering
Munich Network Management Team
Ludwigs Maximilians University

Prof. Dr. Helmut Krcmar
Chair for Information Systems
Technical University of Munich

Prof. Dr. Isabell Welpe
Chair for Strategy and Organisation
Technical University of Munich

Prof. Dr. Jelena Spanjol
Chair for Innovation Management
Ludwigs Maximilians University

Prof. Dr. Jörg Claussen
Chair for Strategy, Technology and Organization
Ludwigs Maximilians University

Prof. Dr. Jörg Eberspächer
Chair for Communication Networks
Technical University of Munich

Prof. Dr. Klaus Diepold
Chair for Data Processing
Technical University of Munich

Prof. Dr. Dr. h.c. Manfred Broy
Chair for Software and Systems Engineering
Technical University of Munich

Prof. Dr. Martin Spann
Chair for Electronic Commerce and Digital Markets
Ludwigs Maximilians University

Prof. Dr. Pramod Bhatotia
Chair for Decentralized Systems Engineering
Technical University of Munich

Prof. Dr. Reiner Braun
Chair for Entrepreneurial Finance
Technical University of Munich

Prof. Dr. Stefanie Rinderle-Ma
Information Systems and Business Process Management
Technical University of Munich

Prof. Dr. Thomas Hess
Chair for Information Systems and New Media
Ludwigs Maximilians University

Prof. Dr. Tobias Kretschmer
Chair for Strategy, Technology and Organization
Ludwigs Maximilians University

Prof. Dr. Wolfgang Kellerer
Chair for Communication Networks
Technical University of Munich

OTHER PUBLICATIONS

2025

The Future of Policy-Enabled Innovation

2024

The Future of Future Software Engineering and IT Operations

2024

The Future of Eldery Care in Nursing Homes

2024

The Future of Utilities in the Era of AI

2023

The Future of Digital Solutions for Sustainable Aviation

2023

The Future of Maritime Shipping

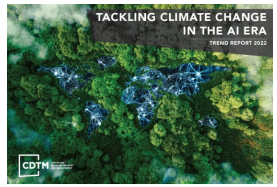
2023

The Future of Communication Technology

2022

The Future of Mittelstand

2022



Tackling Climate Change in the AI Era

SOURCES

[1] Bria, F., Timmers, P., & Gernone, F. (2025, February 13). EuroStack - A European alternative for digital sovereignty. Bertelsmann Stiftung. https://doi.org/10.11586/2025006

[2] Hullin, M. (2025, September 5). Expert Interview with Martin Hullin (Director) from Bertelsmann Stiftung

[3] Sehdev, A., Vanderspar, B., Schiavotto, D., & Schaubroeck, R. (2025, May 21). Technology, media, and telecom in Europe: The new growth engine or another decade of missing out? McKinsey & Company. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/technology-media-and-telecom-in-europe-the-new-growth-engine-or-another-decade-of-missing-out

[4] How competitive is Europe on technology? (2023, July 21). McKinsey & Company. https://www.mckinsey.com/featured-insights/lifting-europes-ambition/videos-and-podcasts/how-competitive-is-europe-on-technology

[5] Erntell, H., Dörner, K., León, M. B., Flötotto, M., & Henz, T. (2024, December 17). European deep tech: What investors and corporations need to know. McKinsey & Company. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/european-deep-tech-what-investors-and-corporations-need-to-know

[6] Sinclair, I., Gagnon, J., Padgett, N., McKinsey, Boardwave, Robinson, P., Sehdev, A., Schaubroeck, R., Apotheker, L., Fernandez, C., Kurgan, S., Murria, V., Padrines, Y., & Courtois, J.-P. (2025). Europe's moonshot moment: Fueling its tech ecosystem for scale. https://www.boardwave.org/boardwave-x-mckinsey-report

[7] Karami, A., & Karami, M. (2025). Edge computing in big data: challenges and benefits. International Journal of Data Science and Analytics. https://doi.org/10.1007/s41060-025-00855-3

[8] Müller, C. (2024). World robotics 2024 – Industrial robots. IFR Statistical Department, VDMA Services GmbH. https://ifr.org/img/worldrobotics/Executive_Summary_WR_2024_Industrial_Robots.pdf

[9] European Commission. (2022, October 12). The Digital Markets Act: ensuring fair and open digital markets. European Commission. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

[10] NIST. (2024, August 13). NIST Releases First 3 Finalized Post-Quantum Encryption Standards | NIST. NIST. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[11] Uusitalo, M. A., Rugeland, P., Boldi, M. R., Strinati, E. C., Demestichas, P., Ericson, M., Fettweis, G. P., Filippou, M. C., Gati, A., Hamon, M.-H., Hoffmann, M., Latva-Aho, M., Pärssinen, A., Richerzhagen, B., Schotten, H., Svensson, T., Wikström, G., Wymeersch, H., Ziegler, V., & Zou, Y. (2021). 6G Vision, Value, Use Cases and Technologies From European 6G Flagship Project Hexa-X. IEEE Access, 9, 160004–160020. https://doi.org/10.1109/ACCESS.2021.3130030

[12] Cherkaoui, S. (2021). Research Landscape – 6G Networks Research in Europe. IEEE Network, 35(6), 4–6. https://doi.org/10.1109/mnet.2021.9687530

[13] Pekkarinen, P. (2025, March 12). Humanoid robot industry – the players and value chain demystified in detail. LinkedIn. https://www.linkedin.com/pulse/humanoid-robot-industry-players-value-chain-detail-petri-pekkarinen-etiff/

[14] Hexa-X-II. (2025, July 1). Results - Hexa-X-II. Hexa-X-II - European Level 6G Flagship Project. https://hexa-x-ii.eu/results/

[15] European Commission. (2025, July 8). European Quantum Communication Infrastructure – EuroQCI. Digital Strategy — Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

[16] European Commission. (n.d.). The next generation Internet of Things. European Commission digital strategy. Retrieved September 27, 2025, from https://digital-strategy.ec.europa.eu/en/policies/next-generation-internet-things

[17] Gill, S. S., Golec, M., Hu, J., Xu, M., Du, J., Wu, H., Walia, G. K., Murugesan, S. S., Ali, B., Kumar, M., Ye, K., Verma, P., Kumar, S., Cuadrado, F., & Uhlig, S. (2024). Edge AI: A Taxonomy, Systematic Review and Future Directions. Cluster Computing, 28(1). https://doi.org/10.1007/s10586-024-04686-y

[18] Eurostat. (2025, August 28). Internet-connected devices are widely used in the EU. Eurostat. https://ec.europa.eu/eurostat/en/web/products-eurostat-news/w/ddn-20250828-2

[19] Huang, T., Huang, W., Zhang, B., Chen, W., & Pan, X. (2025). Optimizing energy consumption in centralized and distributed cloud architectures with a comparative study to increase stability and efficiency. Energy and Buildings, 333, 115454. https://doi.org/10.1016/j.enbuild.2025.115454

[20] 8ra. (n.d.). Multi-Provider Cloud-Edge Continuum. https://www.8ra.com/8ra-community/cloud-edge-continuum/

[21] Precedence Research. (2025, August 21). Edge computing market size to hit USD 5,132.29 Bn by 2034. https://www.precedenceresearch.com/edge-computing-market

[22] European Commission. (n.d.). Europe's digital decade: Digital targets for 2030. Retrieved September 27, 2025, from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

[23] European Commission. (2025, July). Common trust principles for the European data economy. European Commission. https://digital-strategy.ec.europa.eu/en/news/thematic-roadmap-open-source-and-inputs-common-trust-principles

[24] Benkert, L., & Berkov, A. (2025, September 1). Expert Interview with Leonhard Benkert (CEO) and Alexander Berkov (CTO) from DeutschlandGPT.

[25] Rosmaninho, R., Raposo, D., Rito, P., & Sargento, S. (2024, July 24). Edge-cloud continuum orchestration of critical services: A smart-city approach. arXiv. https://arxiv.org/abs/2407.17314

[26] Yee, L., Chui, M., Roberts, R., & Smit, S. (2025, July 22). McKinsey technology trends outlook 2025: The top trends in tech. McKinsey & Company. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech

[27] Computar. (2025). 2025 trends in robotics. https://www.computar.com/blog/2025-trends-in-robotics

[28] Cao, L. (2024). Humanoid robots and humanoid AI: Review, perspectives and directions (Version 2). arXiv. https://arxiv.org/abs/2405.15775v2

[29] Rai, R. (2025). Neural processor market size, share & growth forecast by 2033 [Report]. Straits Research. https://straitsresearch.com/report/neural-processor-market

[30] Allianz Research. (2025, June 11). No country for old robots: How can Europe leap over the robotics tech frontier? Allianz. https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/economic-research/publications/specials/en/2025/june/2025-06-11-Robotics-AZ.pdf

[31] Kavitha, D., & Meher Ujwala, N. R. (2024, May). AI in robotics advancement and applications. International Journal of Research Publication and Reviews, 5(5), 1740–1745. https://ijrpr.com/uploads/V5ISSUE5/IJRPR27298.pdf

[32] Jayanth, R., Gupta, N., & Prasanna, V. (2024). Benchmarking Edge AI platforms for high-performance ML inference [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2409.14803

[33] Sun, L., Rana, K., May, B., Schmeckpeper, K., Suenderhauf, N., Minniti, M. V., & Herlant, L. (2025). Real-is-sim: Bridging the sim-to-real gap with a dynamic digital twin [Preprint]. arXiv. https://arxiv.org/abs/2504.03597

[34] Krug, R. (2025, September 1). Expert Interview with Robert Krug (Research Engineer) from RobCo.

[35] Pikul, J. (2025, June 7). Robots run out of energy long before they run out of work to do — feeding them could change that. The Conversation. https://theconversation.com/robots-run-out-of-energy-long-before-they-run-out-of-work-to-do-feeding-them-could-change-that-255940

[36] Milvus. (2025). What are the computational constraints of edge AI? https://milvus.io/ai-quick-reference/what-are-the-computational-constraints-of-edge-ai

[37] European Commission. (2020, November 3). Open source software strategy. https://commission.europa.eu/about/departments-and-executive-agencies/digital-services/open-source-software-strategy_en

[38] Hoffmann, M., Nagle, F., & Zhou, Y. (2024). The value of open source software (Working Paper No. 24-038). Harvard Business School. https://www.hbs.edu/ris/Publication%20Files/24-038_51f8444f-502c-4139-8bf2-56eb4b65c58a.pdf

[39] Grand View Research. (n.d.). Open Source Services Market Size & Share Report, 2030. https://www.grandviewresearch.com/industry-analysis/open-source-services-market-report

[40] Mordor Intelligence. (n.d.). API management market size & share analysis: Growth trends & forecasts (2025-2030). https://www.mordorintelligence.com/industry-reports/api-management-market

[41] Spencer-Smith, C., & Tomaz, T. (2025). Labour pains: Content moderation challenges in Mastodon growth. Internet Policy Review. https://doi.org/10.14763/2025.1.1831

[42] European Payments Council. (2023). The UPI: Revolutionising real-time digital payments in India. https://www.europeanpaymentscouncil.eu/news-insights/insight/upi-revolutionising-real-time-digital-payments-india

[43] Perlow, J. (2022, March 7). A summary of Census II: Open source software application libraries the world depends on. Linux Foundation. https://www.linuxfoundation.org/blog/blog/a-summary-of-census-ii-open-source-software-application-libraries-the-world-depends-on

[44] European Data Protection Supervisor. (2022, April 28). EDPS launches pilot phase of two social media platforms. https://www.edps.europa.eu/press-publications/press-news/press-releases/2022/edps-launches-pilot-phase-two-social-media

[45] Mastodon gGmbH. (2025). About — Mastodon. Retrieved September 27, 2025, https://joinmastodon.org/about

[46] Dixon, S. (2020, November 24). Instagram: Active users 2018. Statista. https://www.statista.com/statistics/253577/number-of-monthly-active-instagram-users

[47] Çaldağ, M., T., & Gökalp, E. (2023). Understanding barriers affecting the adoption and usage of open access data in the context of organizations. Data and Information Management, 100049–100049. https://doi.org/10.1016/j.dim.2023.100049

[48] Zia, H. B., Raman, A., Castro, I., & Tyson, G. (2025). Collaborative content moderation in the Fediverse. arXiv. https://arxiv.org/pdf/2501.05871 arxiv.org

[49] Microsoft Threat Intelligence. (2023, October). Microsoft digital defense report 2023: Building and improving cyber resilience. Microsoft. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2023

[50] Ivezic, M. (2025, June 24). EU Commission Roadmap Targets 2030 for Post-Quantum Cryptography Transition. PostQuantum - Quantum Computing, Quantum Security, PQC. https://postquantum.com/industry-news/eu-pqc-roadmap

[51] BIS Research. (2025, September 27). Europe Post-Quantum Cryptography Market: Focus on Application, Product, and Regional and Country-Level Analysis - Analysis and Forecast, 2024-2034. Bisresearch.com; BIS Research. https://bisresearch.com/industry-report/europe-post-quantum-cryptography-market.html

[52] Check Point Research. (2025, July 17). Global cyber attacks surge 21% in Q2 2025 — Europe experiences the highest increase of all regions. Check Point Blog. https://blog.checkpoint.com/research/global-cyber-attacks-surge-21-in-q2-2025-europe-experiences-the-highest-increase-of-all-regions/

[53] Vaishnavi. (2025, July 29). What is the impact of quantum computing on encryption and how is post-quantum cryptography evolving to protect data? WebAsha Technologies. https://www.webasha.com/blog/what-is-the-impact-of-quantum-computing-on-encryption-and-how-is-post-quantum-cryptography-evolving-to-protect-data

[54] Irmler, K. (2025, April 4). NIS1 vs NIS2: Unterschied und Hintergrund der Richtlinien. SECJUR. https://www.secjur.com/blog/nis1-vs-nis2

[55] Nobel Prize Outreach. (n.d.). Anton Zeilinger – facts. https://www.nobelprize.org/prizes/physics/2022/zeilinger/facts/

[56] Pichlmayer, B. (2025, September 4). Expert interview with Bernd Pichlmayer (CEO) from FTGG Cyber

[57] Eurelectric. (2024, November 18). A snapshot of cybersecurity in the EU [PDF]. https://www.eurelectric.org/wp-content/uploads/2024/11/A-Eurelectric-snapshot-of-Cybersecurity-2024-11-18-FINAL.pdf

[58] Bradford, S. (2025, September 4). Why are so many organizations dragging their feet on NIS2 compliance? TechRadar. https://www.techradar.com/pro/why-are-so-many-organizations-dragging-their-feet-on-nis2-compliance

[59] Ivezic, M. (2019, October 14). Challenges of Upgrading to Post-Quantum Cryptography (PQC). PostQuantum - Quantum Computing, Quantum Security, PQC. https://postquantum.com/post-quantum/pqc-challenges/

[60] European Union Agency for Cybersecurity (ENISA). (2024, March 27). Foresight cybersecurity threats for 2030: Update 2024. https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024

[61] Trichias, K., Kaloxylos, A., & Willcock, C. (2024). 6G Global Landscape: A Comparative Analysis of 6G Targets and Technological Trends. EuCNC & 6G Summit, 1–6. https://doi.org/10.1109/eucnc/6gsummit60053.2024.10597064

[62] Mohr, W., Kaloxylos, A., Trichias, K., & Willcock, C. (2024). The European Vision for 6G smart networks and services. IEEE Communications Magazine, 62(4), 10–12. https://doi.org/10.1109/mcom.2024.10494954

[63] Pennanen, H., Hänninen, T., Tervo, O., Tölli, A., & Latva-aho, M. (2024). 6G: The Intelligent Network of Everything -- A Comprehensive Vision, Survey, and Tutorial. arXiv. https://doi.org/10.48550/arxiv.2407.09398

[64] Norp, T., Sachdeva, P., Anton, C., Trichias, K., & Mohnani, P. (2024). 6G research & innovation activities in Europe: An overview of EU & nationally funded programmes. https://ezywureyi7i.exactdn.com/wp-content/uploads/2024/07/eucnc24_paper_sns-ice_eu-national-initiatives-vfinal-2.pdf

[65] Lennighan, M. (2023, October 19). EU hands over €130 million for 6G research. Telecoms.com. https://www.telecoms.com/wireless-networking/eu-hands-over-130-million-for-6g-research

[66] Tomás, J. P. (2021, September 23). China accounts for over 40% of 6G patents: report. RCR Wireless. https://www.rcrwireless.com/20210923/5g/china-accounts-over-40-6g-patents-report

[67] Hexa-X-II. (2025, August 4). Hexa-X-II - European level 6G Flagship project. Hexa-X-II - European Level 6G Flagship Project. https://hexa-x-ii.eu/

[68] Madiega, T. & EPRS, European Parliamentary Research Service. (2020). Towards a more resilient EU. In EPRS Ideas Paper [Report]. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

[69] Pohlmann, N., Sparenberg, M., Siromaschenko, I., & Kilden, K. (2014). Secure communication and digital sovereignty in Europe. In Springer eBooks (pp. 155–169). https://doi.org/10.1007/978-3-658-06708-3_12

[70] Eichler, T., & Ziegler, R. (2022, November). Fundamentals of THz technology for 6G (White paper v01.02). Rohde & Schwarz, dataTec AG. https://www.datatec.eu/media/dd/28/9d/1718193632/Rohde-Schwarz_Fundamentals-of-THz-technology-for-6G_v0102_2022-11.pdf

[71] Davies, P. (2025, June 12). Survey: Most Europeans are worried about their digital privacy - and it's impacting how they use AI. Euronews; euronews.com. https://www.euronews.com/next/2025/06/12/survey-most-europeans-are-worried-about-their-digital-privacy-and-its-impacting-how-they-u

[72] Baumann, A., Caprari, L., Dossche, M., Kocharkov, G., & Kouvavas, O. (2025, April 30). How will European consumers react to US tariffs? European Central Bank. https://www.ecb.europa.eu/press/blog/date/2025/html/ecb.blog20250430~a1b1668cda.en.html

[73] Group, S. R. (2025). European Cloud Providers' Local Market Share Now Holds Steady at 15% | Synergy Research Group. Srgresearch.com. https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15

[74] Lange, T. (2025, February 18). Digital skills: The new currency for success in a connected world - Knowledge Innovation Centre. Knowledge Innovation Centre. https://knowledgeinnovation.eu/2025/02/18/digital-skills-the-new-currency-for-success-in-a-connected-world/

[75] Skills for the digital age - Statistics Explained. (2023). Europa.eu. https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=627685

[76] jrice. (2023, June 16). A Talented Home for AI. Sequoia Atlas. https://atlas.sequoiacap.com/a-talented-home-for-ai/

[77] Sherin Shibu. (2025, August 8). Mark Zuckerberg Reportedly Made One Person a $1.5 Billion Job Offer — and Was Rejected. Here's How Google, Microsoft, and OpenAI Are Competing with Meta in the AI Talent Wars. Entrepreneur. https://www.entrepreneur.com/business-news/meta-makes-billion-dollar-job-offer-competing-for-ai-talent/495672

[78] State of the Digital Decade 2025 report. (2025). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/library/state-digital-decade-2025-report

[79] Holzer, B. (2025). Europe appears to be the solution, not the problem. Robert-Schuman.eu. https://www.robert-schuman.eu/en/european-issues/789-europe-appears-to-be-the-solution-not-the-problem

[80] Eurobarometer shows record high trust in the EU, and strong support for the euro and a common defence and security policy. (2025, May 28). Representation in Malta. https://malta.representation.ec.europa.eu/news/eurobarometer-shows-record-high-trust-eu-and-strong-support-euro-and-common-defence-and-security-2025-05-28

[81] Amsterdam, U. van. (2024, May). A Community of Fate: Growing European Identity in Times of Polycrisis. ACES - University of Amsterdam. https://aces.uva.nl/content/news/2024/04/a-new-policy-brief-co-authored-by-theresa-kuhn-aces-theme-group-leader.html?cb

[82] Henley, J. (2023, September 21). Revealed: one in three Europeans now vote anti-establishment. The Guardian. https://www.theguardian.com/world/2023/sep/21/revealed-one-in-three-europeans-now-votes-anti-establishment

[83] Pal, S. (2024). Where is Europe's AI workforce coming from? Interface-Eu.org; interface. https://www.interface-eu.org/publications/where-is-europes-ai-workforce-coming-from

[84] Escritt, T. (2025, June 23). Europeans seek "digital sovereignty" as US tech firms embrace Trump. Reuters. https://www.reuters.com/business/media-telecom/europeans-seek-digital-sovereignty-us-tech-firms-embrace-trump-2025-06-21/

[85] Cassidy, A. (2025, April 8). The Canadians and Danes boycotting American products. BBC. https://www.bbc.com/news/articles/c0el8ed21w9o

[86] Minster, N. (2025, July 3). European businesses are rethinking digital dependencies and placing increased importance on sovereignty in cybersecurity. HarfangLab. https://harfanglab.io/press/european-businesses-are-rethinking-digital-dependencies-and-placing-increased-importance-on-sovereignty-in-cybersecurity/

[87] Reddit - The heart of the internet. (2025). Reddit.com. https://www.reddit.com/r/BuyFromEU/

[88] Go European — Discover European products and services. (2025). Go European. https://www.goeuropean.org/

[89] Brill, J. (2025, February 26). EU Data Boundary. Microsoft on the Issues. https://blogs.microsoft.com/on-the-issues/2025/02/26/microsoft-completes-landmark-eu-data-boundary-offering-enhanced-data-residency-and-transparency/

[90] Frost & Sullivan. (2024). State of the Cloud, Europe, 2024 - Research and Markets. Researchandmarkets.com. https://www.researchandmarkets.com/reports/6164634/state-the-cloud-europe

[91] European Commission. (2025). Eurobarometer. Europa.eu. https://europa.eu/eurobarometer/surveys/detail/3222

[92] Hoheit in Gefahr. (2025, July 23). Exasol. https://www.exasol.com/newsroom/press-releases/hoheit-in-gefahr/

[93] EU launches InvestAI initiative to mobilise €200 billion of investment in artificial intelligence. (2025). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/news/eu-launches-investai-initiative-mobilise-eu200-billion-investment-artificial-intelligence

[94] EU invests €7.3 billion from Horizon Europe to enhance its competitiveness and talent growth. (2025). European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1146

[95] Yanatma, S. (2024, April 8). Skill shortages in Europe: Half of applicants not qualified. Euronews. https://www.euronews.com/business/2024/04/08/eu-jobs-crisis-as-employers-say-applicants-dont-have-the-right-skills

[96] Reuters Staff. (2025, June 18). Sam Altman says Meta offered $100 million bonuses to OpenAI employees. Reuters. https://www.reuters.com/business/sam-altman-says-meta-offered-100-million-bonuses-openai-employees-2025-06-18/

[97] Witze, A. (2025). 75% of US scientists who answered Nature poll consider leaving. Nature, 640. https://doi.org/10.1038/d41586-025-00938-y

[98] Kerr, D. (2025, September 4). Be Best, bots: Melania Trump and tech CEOs discuss saturating US schools with AI. The Guardian; The Guardian. https://www.theguardian.com/us-news/2025/sep/04/melania-trump-artificial-intelligence-schools

[99] European Innovation Council and SMEs Executive Agency - The EU invests in artificial intelligence only 4% of what the U.S. spends on it. (2020). Europa.eu. https://ec.europa.eu/newsroom/eismea/items/864247/en

[100] Minvielle, L. (2024). Are Software Engineer Wages Being Pushed Down? A Report on Tech Salaries. Wearedevelopers.com. https://www.wearedevelopers.com/en/magazine/417/are-software-engineer-wages-being-pushed-down

[101] Coolberth, N. L. (2024, February 13). What State Leaders Need to Know about Measuring Digital Skills: Options and Opportunities. National Skills Coalition. https://nationalskillscoalition.org/blog/future-of-work/what-state-leaders-need-to-know-about-measuring-digital-skills-options-and-opportunities/

[102] EuroStat. (2024, February 22). Digital skills in 2023: impact of education and age - Eurostat. Ec.europa.eu. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240222-1

[103] AN INTERNATIONAL PERSPECTIVE ON DIGITAL LITERACY Results from ICILS 2023. (n.d.). https://www.iea.nl/sites/default/files/2024-11/ICILS_2023_International_Report_0.pdf

[104] OECD. (2023). OECD Skills Outlook 2023. OECD. https://www.oecd.org/en/publications/2023/11/oecd-skills-outlook-2023_df859811.html

[105] What is the Digital Skills Gap? (2025). APMG International. https://apmg-international.com/article/what-digital-skills-gap

[106] Rinceanu, J. (2025). Digital Services Act: Does Internet Regulation Threaten Freedom of Expression? Csl.mpg.de. https://csl.mpg.de/851840/digital-services-act-does-internet-regulation-threaten-freedom-of-expression

[107] Pickard, V. (2019). Democracy without Journalism? Oxford University Press. https://doi.org/10.1093/oso/9780190946753.001.0001

[108] Knafo, S. (n.d.). Report on European technological sovereignty and digital infrastructure | A10-0107/2025 | European Parliament. https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.html

[109] Van den Berg, P. (2022). How the CLOUD-Act works in data storage in Europe. Ncsc.nl. https://english.ncsc.nl/latest/weblog/weblog/2022/how-the-cloud-act-works-in-data-storage-in-europe

[110] SWENSON, A. (2025, January 20). These tech billionaires flanked Trump at inauguration. AP News. https://apnews.com/article/trump-inauguration-tech-billionaires-zuckerberg-musk-wealth-0896bfc3f50d941d62cebc3074267ecd

[111] Quell, M. (2025, May 15). Trump's sanctions on ICC prosecutor have halted tribunal's work. AP News. https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3

[112] The EU's AI Power Play: Between Deregulation and Innovation. (2025). Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation?lang=en

[113] Stanford University. (2025). The 2025 AI Index Report. Stanford.edu. https://hai.stanford.edu/ai-index/2025-ai-index-report

[114] Madiega, T. (2020). BRIEFING EPRS Ideas Paper Towards a more resilient EU. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

[115] Eurostat. (2024, May). Young people - digital world. Ec.europa.eu. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Young_people_-_digital_world

[116] Vanessa. (2025, July 2). Large majority of French, German and Spanish public back tough EU stance on Big Tech, despite risk to Trump relations - People vs. Big Tech. People vs. Big Tech. https://peoplevsbig.tech/large-majority-of-french-german-and-spanish-public-back-tough-eu-stance-on-big-tech-despite-risk-to-trump-relations/

[117] Lobbying power of Amazon, Google and Co. continues to grow | Corporate Europe Observatory. (2023, September 8). Corporateeurope.org. https://corporateeurope.org/en/2023/09/lobbying-power-amazon-google-and-co-continues-grow

[118] Commission fines Google €2.95 billion over abusive practices in online advertising technology. (2025). European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1992

[119] The EU urgently needs technological autonomy from the US, MEPs say. (2025). Science|Business. https://sciencebusiness.net/news/sovereignty/eu-urgently-needs-technological-autonomy-us-meps-say

[120] European AI Act: Opportunities and challenges. (n.d.). Roland Berger. https://www.rolandberger.com/en/Insights/Publications/European-AI-Act-Opportunities-and-challenges.html

[121] Quezada-Tavarez K., Dutkiewicz L., & Krack N. (2022, November 23). Voicing challenges: GDPR and AI research [version 1; peer review: 2 approved with reservations]. Open Res Europe 2022, 2:126. https://doi.org/10.12688/openreseurope.15145.1

[122] European Commission. (2025, April 23). Commission finds Apple and Meta in breach of the Digital Markets Act. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085

[123] Meta Platforms Ireland Ltd. discriminates on the ground of gender when displaying job advertisements to users of Facebook in the Netherlands | College voor de Rechten van de Mens. (2025). Mensenrechten.nl. https://oordelen.mensenrechten.nl/oordeel/2025-17/4a575c22-d4b0-499f-8811-6b5e6720344d

[124] EDPB. (2023, May 22). 1.2 Billion Euro Fine for Facebook as a Result of EDPB Binding Decision | European Data Protection Board. European Data Protection Board. https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

[125] Hurst, A. (2025, April 24). The EU fined Apple and Meta – but failed to really hold them to account. Was that to appease Trump? The Guardian; The Guardian. https://www.theguardian.com/commentisfree/2025/apr/24/the-eu-fined-apple-and-meta-but-failed-to-really-hold-them-to-account-was-that-to-appease-trump

[126] Eurobarometer. (2019). Europa.eu. https://europa.eu/eurobarometer/surveys/detail/2253

[127] Santi Amantini, L. (2021). Populist Anti-immigrant Sentiments Taken Seriously: A Realistic Approach. Res Publica, 28(1). https://doi.org/10.1007/s11158-021-09516-1

[128] Hoffmann, I. (2024, November 22). eupinions - Europeans prefer greater independence from the US. Bertelsmann-Stiftung.de. https://www.bertelsmann-stiftung.de/en/topics/latest-news/2024/november/europeans-prefer-greater-independence-from-the-us

[129] Green, R. (2024, September 30). The Year of elections: the Rise of Europe's Far Right. Ibanet.org; International Bar Association. https://www.ibanet.org/The-year-of-elections-The-rise-of-Europes-far-right

[130] Calabresi, M. (2025, July 24). Where Giorgia Meloni Is Leading Europe. Time. https://time.com/7304882/giorgia-meloni-interview

[131] European Parliament. (2025, March 25). Survey confirms Europe's citizens want the EU to protect them and act in unity | News | European Parliament. Europa.eu. https://www.europarl.europa.eu/news/en/press-room/20250317IPR27385/survey-confirms-europe-s-citizens-want-the-eu-to-protect-them-and-act-in-unity

[132] L. Guiso, Herrera, H., Morelli, M., & T. Sonno. (2024). Economic Insecurity and the Demand for Populism in Europe. Economica, 91(362). https://doi.org/10.1111/ecca.12513

[133] Kiderlin, S. (2024, April 29). Germany's far-right AfD party is finding success on TikTok — as its popularity among young voters grows. CNBC. https://www.cnbc.com/2024/04/29/germanys-afd-is-finding-success-on-tiktok-as-its-youth-vote-grows.html

[134] European Values Study. (2025, January 14). https://europeanvaluesstudy.eu/about-evs/research-topics/identity/

[135] Matafora, B., Ziemes, J. F., & Abs, H. J. (2023). A multilevel analysis of factors influencing teenagers' identification with Europe: the effects of migration and learning opportunities. Comparative Migration Studies, 11(1). https://doi.org/10.1186/s40878-023-00348-x

[136] Végh, Z. (2019). Central Europe's Radical Right and EU Foreign Policy. GMFUS. https://www.gmfus.org/news/central-europes-radical-right-and-eu-foreign-policy

[137] Giudici, A., Gruber, O., Schnell, P., & Pultar, A. (2024). Far-right parties and the politics of education in Europe. Journal of Contemporary European Studies, 33(1), 1–14. https://doi.org/10.1080/14782804.2024.2352518

[138] Murche, L. (2025, March 20). Europe under pressure to act: Digital sovereignty in the public sector. Smart Country Convention. Retrieved September 28, 2025, https://www.smartcountry.berlin/en/newsblog/europe-under-pressure-to-act-digital-sovereignty-in-the-public-sector.html

[139] European Central Bank. (2025, February). Report on card schemes and processors. https://www.ecb.europa.eu/pub/pdf/other/ecb.reportcardschemes202502~1614226b0a0a.en.pdf

[140] Reuters. (2025, September 24). Disruptions drag on at Berlin airport after cyberattack. Retrieved September 28, 2025, https://www.reuters.com/business/aerospace-defense/disruptions-drag-berlin-airport-after-cyberattack-2025-09-24/

[141] Michels, J. D. (2025, February 18). Sovereign Cloud for Europe: Independent Research Report prepared for Broadcom (SSRN Scholarly Paper No. 5146122). SSRN. https://ssrn.com/abstract=5146122

[142] European Investment Bank. (2024). Investment barriers in the European Union 2023: A report by the European Investment Bank Group. https://www.eib.org/attachments/lucalli/20230330_investment_barriers_in_the_eu_2023_en.pdf

[143] European Commission. (2025, June 16). 2025 State of the Digital Decade package. Shaping Europe's Digital Future. Retrieved September 28, 2025, https://digital-strategy.ec.europa.eu/en/policies/2025-state-digital-decade-package

[144] Secomea. (2025, July 8). NIS2 compliance in Europe: Country-by-country updates for manufacturers and critical infrastructure (2025-2026). Retrieved September 29, 2025, https://secomea.com/blog/compliance/nis2-compliance-in-europe-country-by-country/

[145] European Commission. (n.d.). Europe's Digital Decade. Retrieved September 28, 2025, https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade

[146] Hulkó, G., Kálmán, J., & Lapsánszky, A. (2025, February 5). The politics of digital sovereignty and the European Union's legislation: Navigating crises. Frontiers in Political Science, 7. https://doi.org/10.3389/fpos.2025.1548562

[147] Future of Life Institute. (2024, February 27). High-level summary of the AI Act (updated May 30). Retrieved September 29, 2025, https://artificialintelligenceact.eu/high-level-summary/

[148] European Insurance and Occupational Pensions Authority. (n.d.). Digital Operational Resilience Act (DORA). Retrieved September 29, 2025, https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

[149] EUR-Lex - 32023C0123(01) - EN - EUR-Lex. (2023). Europa.eu. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOC_2023_023_R_0001

[150] European Commission. (2023, June 28). Proposal for a directive on payment services and electronic money services in the internal market (COM/2023/366 final) [Proposal for a directive of the European Parliament and of the Council, 2023/0209 (COD)]. EUR-Lex. Retrieved September 29, 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023PC0366

[151] Cannataci, J., Fehrensen, B., Lucke, B., & Gütschow, M. (2025, March). The digital euro: An analysis of the Commission's proposed legislation [PDF]. Universität Hamburg. https://www.wiso.uni-hamburg.de/fachbereich-vwl/professuren/lucke/bilder/the-commission-s-proposal-for-a-digital-euro-bl-13-3-25.pdf

[152] Dual-use and defence in Horizon Europe: European Commission's new approach is unacceptable | LERU. (2025). LERU. https://www.leru.org/news/dual-use-and-defence-in-horizon-europe-this-is-not-the-way-to-go

[153] Council of Europe. (n.d.). Digital Governance – Overview. Retrieved September 29, 2025, https://www.coe.int/en/web/digital-governance/overview

[154] Baghal-Schmid, A., & Esser, L. (2025, May 13). Numbers and figures: GDPR Enforcement Tracker Report 2024/2025. CMS. Retrieved September 29, 2025, https://cms.law/en/int/publication/gdpr-enforcement-tracker-report/numbers-and-figures

[155] EU-INC. (n.d.). Let's create the ideal EU-Inc for Europe – together. Retrieved September 29, 2025, https://proposal.eu-inc.org/14d076fd79c581199761dd7e8b020774?v=14d076fd79c58146b048000caeed686a

[156] European Commission. (2025, May 28). Commission staff working document: Accompanying the notification — The EU Startup and Scaleup Strategy: Choose Europe to start and scale (SWD (2025) 138 final). https://research-and-innovation.ec.europa.eu/document/download/8f899486-6e4e-48df-8633-9582375f41eb_en

[157] Adomaitis, N., & Ahlander, J. (2025, August 21). What is known about the Nord Stream gas pipeline explosions? Reuters. Retrieved September 29, 2025, https://www.reuters.com/world/europe/what-is-known-about-nord-stream-gas-pipeline-explosions-2025-08-21/

[158] European Parliament. (2023, February 15). Chips Act – the EU's plan to overcome semiconductor shortage. Retrieved September 29, 2025, https://www.europarl.europa.eu/topics/en/article/20230210STO74502/chips-act-the-eu-s-plan-to-overcome-semiconductor-shortage

[159] Bundesinstitut für Bau-, Stadt- und Raumforschung. (n.d.). Network cross-border data. Retrieved September 29, 2025, https://www.bbsr.bund.de/BBSR/EN/research/specialist-articles/spatial-development/network-crossborderdata/main.html

[160] Jahangir, R. (2025, April 24). What's behind Europe's push to "simplify" tech regulation? TechPolicy.Press. Retrieved September 29, 2025, https://www.techpolicy.press/whats-behind-europes-push-to-simplify-tech-regulation/

[161] European Data Protection Board. (2024, April). EDPB Strategy 2024-2027 (Edinburgh). Retrieved September 29, 2025, https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf

[162] Navid K. (2022). How Many Single Rulebooks? The EU's Patchwork Approach to Ensuring Regulatory Consistency in the Area of Investment Management. European Business Organization Law Review, 23(2), 347–390. https://doi.org/10.1007/s40804-021-00228-w

[163] Youngs, R. (2025, June 16). Rethinking EU digital policies: From tech sovereignty to tech citizenship. Carnegie Endowment for International Peace. Retrieved September 29, 2025, https://carnegieendowment.org/research/2025/06/rethinking-eu-digital-policies-from-tech-sovereignty-to-tech-citizenship?lang=en

[164] European Commission. (2020). Shaping Europe's Digital Future. https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf

[165] Teevan, C., & Pouyé, R. (2024, December 11). Tech sovereignty and a new EU foreign economic policy [Brief]. ECDPM. Retrieved September 29, 2025, https://ecdpm.org/work/tech-sovereignty-and-new-eu-foreign-economic-policy

[166] European Policy Centre & Konrad-Adenauer-Stiftung. (2020). Digital SA paper EPC and KAS [PDF]. https://d1xp398qalq39s.cloudfront.net/content/PDF/2020/Digital_SA_paper_EPC_and_KAS.pdf

[167] Follin, A. (2025, February 4). Digital sovereignty in Europe: Navigating the challenges of the digital era. ESCP International Politics Society. Retrieved September 29, 2025, https://pppescp.com/2025/02/04/digital-sovereignty-in-europe-navigating-the-challenges-of-the-digital-era/

[168] European Commission. (2025, August 1). AI Act: Regulatory framework for artificial intelligence. Retrieved September 29, 2025, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

[169] Amazon Web Services. (n.d.). Europäische digitale Souveränität – Amazon Web Services [Digital sovereignty in Europe]. Retrieved September 29, 2025, https://aws.amazon.com/de/compliance/europe-digital-sovereignty/

[170] Going Digital to Advance Data Governance for Growth and Well-being. (2025). OECD. https://www.oecd.org/en/publications/going-digital-to-advance-data-governance-for-growth-and-well-being_e3d783b0-en.html

[171] EuroStack. (2025, February 4). Gaia-X — Chronicle of a failure foretold. Retrieved September 29, 2025, https://euro-stack.com/blog/2025/2/gaia-x-failure

[172] Frey, C. B., Presidente, G., & Andres, P. (2025, January 5). Redirecting AI: Privacy regulation and the future of artificial intelligence [VoxEU column]. CEPR. Retrieved September 29, 2025, https://cepr.org/voxeu/columns/redirecting-ai-privacy-regulation-and-future-artificial-intelligence

[173] Cloud computing | Shaping Europe's digital future. (n.d.). Digital-Strategy.ec.europa.eu. https://digital-strategy.ec.europa.eu/en/policies/cloud-computing

[174] European Commission. (2025). Cyber Resilience Act | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[175] St. Aubin, C., & Liedke, J. (2023, July 20). Most Americans favor restrictions on false information and violent content online. Pew Research Center. https://www.pewresearch.org/short-reads/2023/07/20/most-americans-favor-restrictions-on-false-information-violent-content-online/

[176] steffennachmorgen. (2023, August 9). New Study: Attitudes and Perceptions of Disinformation in Europe - Upgrade Democracy. Upgrade Democracy. https://upgradedemocracy.de/en/new-study-attitudes-and-perceptions-of-disinformation-in-europe/

[177] Chiara, P. G. (2025). Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise? European Journal of Risk Regulation, 1–16. https://doi.org/10.1017/err.2025.9

[178] Lane, P. R. (2025). The digital euro: Maintaining the autonomy of the monetary system (SUERF Policy Note No. 369). SUERF - The European Money and Finance Forum. https://www.suerf.org/wp-content/uploads/2025/04/SUERF-Policy-Note-369_-Lane.pdf

[179] Bank, E. C. (2025, September 4). The digital euro: ensuring resilience and inclusion in digital payments. European Central Bank. https://www.ecb.europa.eu/press/key/date/2025/html/ecb.sp250904~70ab593276.en.html

[180] Wero. (n.d.). Wero – Digital payment wallet. Retrieved September 29, 2025, https://wero-wallet.eu/

[181] European Union. (n.d.). European crypto-assets regulation (MiCA). EUR-Lex. Retrieved September 29, 2025, https://eur-lex.europa.eu/EN/legal-content/summary/european-crypto-assets-regulation-mica.html

[182] European Central Bank. (n.d.). Our retail payments strategy. Retrieved September 30, 2025, https://www.ecb.europa.eu/paym/integration/retail/retail_payments_strategy/html/index.en.html

[183] Bezemer, D., Sanders, M., Kramer, B., & Simić, A. (2025). Stablecoins and digital euro: Friends or foes of European monetary policy? European Parliament, Economic Governance and EMU Scrutiny Unit. https://www.europarl.europa.eu/cmsdata/296480/MD_SFL%20June%202025_FINAL.pdf

[184] Eurofi. (2024, December). Digital Euro: Features and Challenges [PDF]. https://www.eurofi.net/wp-content/uploads/2024/12/iv.3-digital-euro-features-and-challenges.pdf

[185] Kumar, A., Chhangani, A., Lassiter, J., & Haar, K. (2024, April 10). Standards and interoperability: The future of the global financial system [Issue brief]. Atlantic Council. Retrieved September 30, 2025, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/standards-and-interoperability-the-future-of-the-global-financial-system/

[186] European Central Bank. (n.d.). Cross-border payments [Webpage]. Retrieved September 30, 2025, https://www.ecb.europa.eu/paym/target/tips/crossborder/html/index.en.html

[187] European Commission. (2024, January 24). On options for enhancing support for research and development involving technologies with dual-use potential. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52024DC0027

[188] Hui, W. (2025). Convergent technologies in autonomous weapons systems. Canadian Global Affairs Institute. https://www.cigionline.org/documents/3446/DPH-paper-Hui.pdf

[189] European Commission. (2021). Horizon Europe. European Commission. https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

[190] Butcher, M. (2024, September 26). As war rages in Ukraine, investment in European defense and dual-use tech skyrockets | TechCrunch. TechCrunch. https://techcrunch.com/2024/09/26/as-war-rages-in-ukraine-investment-in-european-defense-and-dual-use-tech-skyrockets/

[191] A pivotal moment for European strategic autonomy, courtesy of Trump | Lowy Institute. (2025). Lowyinstitute.org. https://www.lowyinstitute.org/the-interpreter/pivotal-moment-european-strategic-autonomy-courtesy-trump

[192] Konrad Wolfenstein. (2025, August 29). Dual-use economy: Why the invisible power of dual-use technology will determine Europe's future. Xpert.Digital. https://xpert.digital/en/dual-use-economy/

[193] European Parliamentary Research Service. (2025, April). Defence and artificial intelligence (EPRS Briefing No. 769580). European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf

[194] 2025 Update of the EU Control List of Dual-Use Items. (2025, September 8). Trade and Economic Security. https://policy.trade.ec.europa.eu/news/2025-update-eu-control-list-dual-use-items-2025-09-08_en

[195] CompaniesMarketCap. (2025). NVIDIA (NVDA) - Market capitalization. CompaniesMarketCap. Retrieved September 8, 2025, https://companiesmarketcap.com/nvidia/marketcap/

[196] Largest DAX companies by market cap. (n.d.). Companiesmarketcap.com. https://companiesmarketcap.com/dax/largest-companies-by-market-cap/

[197] García-Santana, M., & Moral-Benito, E. (2025). Recent global shocks: consequences and policies. SERIEs. https://doi.org/10.1007/s13209-025-00313-0

[198] Sturgeon, T. J. (2021). Upgrading strategies for the digital economy. Global Strategy Journal, 11(1), 34–57. https://doi.org/10.1002/gsj.1364

[199] Gantner, C. (2025, March 24). Gaia-X and Partners to Showcase Cross-Border Data Collaboration at Hannover Messe 2025. Gaia-X.eu. https://gaia-x.eu/gaia-x-and-partners-to-showcase-cross-border-data-collaboration-at-hannover-messe-2025/

[200] Ilzetzki, E. (2023). Guns and Growth: The Economic Consequences of Defense Buildups. Kiel Institute for the World Economy. https://www.ifw-kiel.de/publications/guns-and-growth-the-economic-consequences-of-defense-buildups-33747/

[201] Demertzis, M., Pinkus, D., & Ruer, N. (2024). Accelerating strategic investment in the European Union beyond 2026. Bruegel Report, 1(24), 2024-01.

[202] G20 Digital Economy Task Force. (2016). G20 digital economy development and cooperation initiative. Ministry of Foreign Affairs of Japan. https://www.mofa.go.jp/files/000185874.pdf

[203] Rong, K. (2022). Research agenda for the digital economy. Journal of Digital Economy, 1(1), 20–31. https://doi.org/10.1016/j.jdec.2022.08.004

[204] O'Grady, M. (2024, July 23). The Global Digital Economy Will Reach $16.5 Trillion And Capture 17% Of Global GDP By 2028. Forrester. https://www.forrester.com/blogs/the-global-digital-economy-will-reach-16-5-trillion-and-capture-17-of-global-gdp-by-2028/

[205] DataReportal, Meltwater, & We Are Social. (2025, February 5). Number of internet and social media users worldwide as of February 2025 (in billions) [Graph]. In Statista. Retrieved August 31, 2025, https://www.statista.com/statistics/617136/digital-population-worldwide/

[206] Transforma Insights. (2025, September 5). Current IoT forecast highlights. Transforma Insights. https://transformainsights.com/research/forecast/highlights

[207] European Parliament, & Council of the European Union. (2022). Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030. Official Journal of the European Union, L 323, 4–26. http://data.europa.eu/eli/dec/2022/2481/oj

[208] Transforma Insights. (2020, May 20). Global IoT market to grow to $1.5trn annual revenue by 2030 | IoT Now news & reports. IoT Now News – How to Run an IoT Enabled Business. https://www.iot-now.com/2020/05/20/102937-global-iot-market-to-grow-to-1-5trn-annual-revenue-by-2030/

[209] Organisation for Economic Co-operation and Development. (2024). OECD digital economy outlook 2024 (Vol. 1): Embracing the technology frontier. OECD Publishing. https://doi.org/10.1787/a1689dc5-en

[210] Statista. (2025). Artificial intelligence – worldwide. Statista. https://www.statista.com/outlook/tmo/artificial-intelligence/worldwide.

[211] Robinson, D. (2025, July 28). "Impossible hill to climb": US clouds crush European competition on their home turf. Theregister.com; The Register. https://www.theregister.com/2025/07/28/euro_cloud_vs_us/

[212] Niebel, T., O'Mahony, M., & Saam, M. (2017). The contribution of intangible assets to sectoral productivity growth in the EU. Review of Income and Wealth, 63(S1), S49–S67. https://doi.org/10.1111/roiw.12248

[213] Collet, M. (2025, June 11). Polytechnique Insights. https://www.polytechnique-insights.com/en/columns/digital/can-gafams-be-taxed-more-the-true-the-false-and-the-uncertain/

[214] European Economic and Social Committee. (2023). Opinion of the European Economic and Social Committee — Digital sovereignty: A crucial pillar for EU's digitalisation and growth (Own-initiative opinion, INT/980-EESC-2022-02134).Official Journal of the European Union, C 75, 8–12

[215] Bauer, H., Burkacky, O., Kenevan, P., Mahindroo, A., & Patel, M. (2020). Coronavirus: Implications for the semiconductor industry The coronavirus is shifting demand patterns for major semiconductor end markets. How will these changes ultimately affect the semiconductor industry, and how can leaders respond? https://www.mckinsey.com/~/media/McKinsey/Industries/Semiconductors/Our%20Insights/Coronavirus%20Implications%20for%20the%20semiconductor%20industry/Coronavirus-Implications-for-the-semiconductor-industry.pdf

[216] Hérault, P. (2021, December). Strengthening sovereignty in the era of global value chains (Études de l'Ifri). Institut français des relations internationales (Ifri). Translated by Cadenza Academic Translations.

[217] Arjona, R., Connell Garcia, W., & Herghelegiu, C. (2025, April 3). EU supply chain tectonics. VoxEU, CEPR. https://cepr.org/voxeu/columns/eu-supply-chain-tectonics

[218] Glencross, A. (2024). The geopolitics of supply chains: EU efforts to ensure security of supply. Global Policy, 15(4), 729–739. https://doi.org/10.1111/1758-5899.13388

[219] European Investment Ban, & DG GROW. (2024). Navigating Supply Chain Disruptions: New Insights into the Resilience and Transformation of EU Firms. European Investment Bank. Retrieved August 31, 2025, https://www.developmentaid.org/api/frontend/cms/file/2024/10/20240179_navigating_supply_chain_disruptions_en.pdf

[220] Porsche Consulting. (2021). Modularization in industrial goods: A framework to master increasing complexity. Porsche Consulting.

[221] Overvest, M. (2022, March 3). Supply Chain Statistics – 18 Key Figures of 2022. Procurement Tactics. https://procurementtactics.com/supply-chain-statistics/

[222] Operating resilient supply chains. (n.d.). Retrieved September 29, 2025, https://geodis.com/sites/default/files/2021-07/GEODIS%20RA_RSE_2020_UK.pdf

[223] Mykyta, S. (2025). Global Trends in Logistics: The Impact of Geopolitical Factors on Supply Chains. The American Journal of Management and Economics Innovations, 07(03), 46–55. https://doi.org/10.37547/tajmei/Volume07Issue03-07

[224] Allianz Research. (2025). Semiconductors – Europe's billion-dollar question: How to close the gap with the US and Asia. Allianz SE. https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/economic-research/publications/specials/en/2025/march/2025-03-06-Semiconductors.pdf

[225] European Commission. (2025). State of the Digital Decade 2025 package. Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/2025-state-digital-decade-package

[226] Global Professional Services International (GPSI). (2025, April 9). Cybersecurity in supply chain management: Navigating the digital frontier. GPSI. https://www.gpsi-intl.com/blog/cybersecurity-in-supply-chain-management/

[227] De Gregorio, G., & Radu, R. (2022). Digital constitutionalism in the new era of Internet governance. International Journal of Law and Information Technology, 30(1), 68–87. https://doi.org/10.1093/ijlit/eaac004

[228] Tardieu, H. (2022). Role of Gaia-X in the European Data Space Ecosystem. In B. Otto, M. ten Hompel, & S. Wrobel (Eds.), Designing Data Spaces (pp. 41–59). Springer. https://doi.org/10.1007/978-3-030-93975-5_4

[229] Raasch, P. (2025, July 10). Why BMW, Mercedes, VW suddenly team up to build software together. The German Autopreneur. https://germanautopreneur.com/p/bmw-mercedes-vw-software-alliance

[230] TUM Think Tank. (n.d.). Turning digital sovereignty-in-the-cloud from theory to action. https://tumthinktank.de/en/project/turning-digital-sovereignty-in-the-cloud-from-theory-to-action/

[231] VITAKO – Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e. V. (Hrsg.). (2025). VITAKO aktuell, 01|2025. ISSN 2194-1165. Retrieved September 6, 2025, https://vitako.de/wp-content/uploads/2025/03/VA25_01_web.pdf

[232] Federal Ministry for Economic Affairs and Energy (BMWi). (2020). GAIA-X: Driver of digital innovation in Europe – Featuring the next generation of data infrastructure. https://www.bundeswirtschaftsministerium.de/Redaktion/EN/Publikationen/gaia-x-driver-of-digital-innovation-in-europe.pdf?__blob=publicationFile&v=1

[233] Science Europe. (2024, September 26). Research funding at the forefront of EU strategy in the Draghi Report. Retrieved September 8, 2025, https://scienceeurope.org/news/research-funding-at-the-forefront-of-eu-strategy-in-the-draghi-report/

[234] Omarini, A. (2022). The changing landscape of retail banking and the future of digital banking. In The Future of Financial Systems in the Digital Age: Perspectives from Europe and Japan (pp. 133-158). Singapore: Springer Singapore.

[235] Robinson, D. K., Simone, A., & Mazzonetto, M. (2021). RRI legacies: co-creation for responsible, equitable and fair innovation in Horizon Europe. Journal of Responsible Innovation, 8(2), 209-216.

[236] Sanni, M. A. (2025). Entrepreneurship and Innovation in Enhancing Public-Private Partnership Effectiveness for Unlocking Economic Potential. In Public Private Partnership Dynamics for Economic Development (pp. 213-242). IGI Global Scientific Publishing.

[237] McKinsey & Company (2025), European defense tech start-ups: In it for the long run? . https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/european-defense-tech-start-ups-in-it-for-the-long-run

[238] Dealroom.co. (2015). https://app.dealroom.co/companies/quantum_systems

[239] Dealroom.co. (2024). https://app.dealroom.co/companies/helsing

[240] Goldman Sachs Global Institute. (2025). The Future of European Defense. Goldman Sachs. https://www.goldmansachs.com/insights/articles/the-future-of-european-defense

[241] European Defence Agency. (2025, September 2). EU defence spending hits €343 billion in 2024, EDA data shows. European Defence Agency. https://eda.europa.eu/news-and-events/news/2025/09/02/eu-defence-spending-hits-343-bln-in-2024-eda-data-shows

[242] NATO. (2025). Deterrence and defence. https://www.nato.int/cps/en/natolive/topics_133127.htm

[243] European Parliamentary Research Service. (2025). ReArm Europe Plan/Readiness 2030. PE 769.566. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769566/EPRS_BRI(2025)769566_EN.pdf

[244] NATO Parliamentary Assembly. (2025). Mastering the future of uncrewed warfare (Report No. 023 STCTTS 25 E Rev.1). NATO Parliamentary Assembly

[245] Matthijs, M. (2025, July 30). U.S.-EU Trade Deal Avoids a Tariff War, but Deepens European Dependence. Council on Foreign Relations. https://www.cfr.org/article/us-eu-trade-deal-avoids-tariff-war-deepens-european-dependence

[246] Losey, S. (2022, March 16). Full weapons tester report highlights F-35 availability, software problems. Defense News. https://www.defensenews.com/air/2022/03/16/full-weapons-tester-report-highlights-f-35-availability-software-problems/

[247] Stockholm Internationa Peace Research Institute. (2025, March 10). Ukraine the world's biggest arms importer; United States' dominance of global arms exports grows as Russian exports continue to fall. SIPRI. https://www.sipri.org/media/press-release/2025/ukraine-worlds-biggest-arms-importer-united-states-dominance-global-arms-exports-grows-russian

[248] Chinn, D., Stöber, J., Fischer, H., Köhler, J., Wagner, K., & Grießmann, N. (2025, February 12). European defense tech start-ups: In it for the long run? McKinsey & Company. https://www.mckinsey.de/industries/aerospace-and-defense/our-insights/european-defense-tech-start-ups-in-it-for-the-long-run

[249] European Commission. (2025). The economic impact of higher defence spending. Economy and Finance. https://economy-finance.ec.europa.eu/economic-forecast-and-surveys/economic-forecasts/spring-2025-economic-forecast-moderate-growth-amid-global-economic-uncertainty/economic-impact-higher-defence-spending_en

[250] European Central Bank. (2025). Fiscal aspects of European defence spending: implications for euro area macroeconomic projections and associated risks. ECB Economic Bulletin, Issue 5/2025. https://www.ecb.europa.eu/press/economic-bulletin/focus/2025/html/ecb.ebbox202505_07~d1ab88c6b1.en.html

[251] European Commission. (2023). European Innovation Council (EIC) Fund: An introduction. Publications Office of the European Union https://research-and-innovation.ec.europa.eu/document/download/8f899486-6e4e-48df-8633-9582375f41eb_en

[252] European Commission. (n.d.). 2025 State of the Digital Decade package. https://digital-strategy.ec.europa.eu/en/policies/2025-state-digital-decade-package

[253] European Investment Bank. (2024). The scale-up gap: Financial market constraints holding back innovative firms in the European Union. https://www.eib.org/attachments/lucalli/20240130_the_scale_up_gap_en.pdf

[254] European Commission. (2024). The future of European competitiveness — Part A (COM(2024) 97 final). Publications Office of the European Union. https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en

[255] Quas, A., Mason, C., Scellato, G., & Gornall, W. (2022). The scale-up finance gap in the EU. Small Business Economics, 59(2), 487–506. https://pmc.ncbi.nlm.nih.gov/articles/PMC9707731/

[256] Actuia. (2022, November 10). Climate tech start-up Kayrros backed by the French Tech Souveraineté fund in a €40 million financing round. https://www.actuia.com/en/news/climate-tech-start-up-kayrros-backed-by-the-french-tech-souverainete-fund-in-a-e40-million-financing-round/

[257] Bundesministerium für Wirtschaft und Klimaschutz. (2022, October 18). The Sovereign Tech Fund launches: Funding an investment in Europe's digital sovereignty [Press release]. BMWK.https://www.bundeswirtschaftsministerium.de/Redaktion/EN/Pressemitteilung en/2022/10/20221018-the-sovereign-tech-fund-launches-funding-an-investment-in-europes-digital-sovereignty.html

[258] Moloney, N. (2016). Capital Markets Union: A reality check. European Capital Markets Institute Policy Paper.

[259] Gernone, F., Bria, F., & Timmers, P. (2025). EuroStack–A European Alternative for Digital Sovereignty. Bertelsmann Stiftung. Gütersloh.

[260] Dachs, B. (2023). The European Chips Act (No. 58). FIW-Kurzbericht.

[261] European Chips Skills Academy. (2024). ECSA skills strategy 2024: Building Europe's semiconductor talent pipeline. Chips Academy. https://chipsacademy.eu/wp-content/uploads/2024/11/ECSA-Skills-Strategy-2024.pdf

[262] European Commission. (2024, January 24). Commission launches AI innovation package to support Artificial Intelligence startups and SMEs | Shaping Europe's digital future. Digital-Strategy.ec.europa.eu. https://digital-strategy.ec.europa.eu/en/news/commission-launches-ai-innovation-package-support-artificial-intelligence-startups-and-smes

[263] Brown, R., Mawson, S., & Rowe, A. (2019). Start-ups, scale-ups and unicorns: Towards a new typology of high-growth firms. International Small Business Journal, 37(3), 227–248.https://www.researchgate.net/publication/378994199_Scale-ups_and_High-Growth_Firms_Theory_Definitions_and_Measurement

[264] Crespi, F., Caravella, S., Menghini, M., & Salvatori, C. (2021). European technological sovereignty: an emerging framework for policy strategy. Intereconomics, 56(6), 348-354.

[265] IPCC. (2022). Climate Change 2022: Impacts, Adaptation and Vulnerability — Technical Summary (AR6 WGII). https://www.ipcc.ch/report/ar6/wg2/downloads/report/IPCC_AR6_WGII_TechnicalSummary.pdf

[266] Baskaran, G., & Schwartz, M. (2025, July 28). Developing Rare Earth Processing Hubs: An Analytical Approach (CSIS Analysis). https://www.csis.org/analysis/developing-rare-earth-processing-hubs-analytical-approach

[267] Eurostat. (2025). Shedding light on energy in Europe – 2025 edition. https://ec.europa.eu/eurostat/de/web/interactive-publications/energy-2025

[268] European Commission. (2023). Critical Raw Materials Act. https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials/critical-raw-materials-act_en

[269] Rzepecka, J., Fuksiewicz, A., Squillante, F., Alijošius, L., Godlovitch, I., Stamm, P., Wielgosch, J., & Lundborg, M. (2024). The impact of EU legislation in the area of digital and green transition, particularly on SMEs: Study requested by the IMCO Committee. Publications Office of the European Union. https://doi.org/10.2861/5296842

[270] European Commission. (2025, July 15). In focus: Reaching the EU's energy efficiency target. https://energy.ec.europa.eu/news/focus-reaching-eus-energy-efficiency-target-2025-07-15_en

[271] Masanet, E., Shehabi, A., & Koomey, J. (2025). Data centre energy use: Critical review of models and results. IEA 4E Technology Collaboration Programme. https://www.iea-4e.org/wp-content/uploads/2025/05/Data-Centre-Energy-Use-Critical-Review-of-Models-and-Results.pdf

[272] Ember. (2025, June). Grids for data centres in Europe. Ember. https://ember-energy.org/app/uploads/2025/06/Grids-for-data-centres-in-Europe.pdf

[273] European Commission. (2019). Brownfield redevelopment in Europe. Publications Office of the European Union. https://commission.europa.eu/system/files/2019-04/brownfield_conference_report_0.pdf

[274] AlgorithmWatch. (2023, August 10). Infrastructure or intrusion? Europe's conflicted data centre expansion. AlgorithmWatch. https://algorithmwatch.org/en/infrastructure-intrusion-conflict-data-center/

[275] European Commission. (n.d.). Corporate sustainability reporting (CSRD). Retrieved August 31, 2025, https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en

[276] Commission Delegated Regulation (EU) 2023/2772 of 31 July 2023 supplementing Directive 2013/34/EU as regards European Sustainability Reporting Standards (ESRS). (2023). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg_del/2023/2772/oj/eng

[277] European Commission. (n.d.). Energy Efficiency Directive. Retrieved August 31, 2025, https://energy.ec.europa.eu/topics/energy-efficiency/energy-efficiency-targets-directive-and-rules/energy-efficiency-directive_en

[278] Commission Delegated Regulation (EU) 2024/1364 of 14 March 2024 on the first phase of a Union rating scheme for data centres (reporting mechanism and KPIs). (2024). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401364

[279] Grant Thornton. (2024, December 4). CSRD reporting: What you need to know. https://www.grantthornton.com/insights/articles/esg/2023/csrd-reporting-what-you-need-to-know?

[280] European Commission. (o. J.). The European Green Deal. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en

[281] ClientEarth. (2025, July 7). Non-compliance with environmental laws harms society and nature — transparency is key to closing the gap. https://www.clientearth.org/latest/news/non-compliance-with-environmental-laws-harms-society-and-nature/

[282] Regulation (EU) 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act). (2023). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng

[283] European Commission. (2025, July 24). Data Act explained. https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

[284] International Organization for Standardization. (2023). ISO/IEC 42001:2023—Information technology—Artificial intelligence—Management system. Retrieved August 31, 2025, https://www.iso.org/obp/ui/en/

[285] Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act). (2024). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

[286] European Commission. (n.d.). Digital skills—Shaping Europe's digital future. Retrieved August 31, 2025, https://digital-strategy.ec.europa.eu/en/policies/digital-skills

[287] Eurostat. (2024). Towards Digital Decade targets for Europe (Statistics Explained). Eurostat. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Towards_Digital_Decade_targets_for_Europe

[288] Hsu, J. (2025). A comparative examination of AI regulation in the European Union. Pittsburgh Undergraduate Review, 16(2), 123–147. https://www.pur.pitt.edu/pur/article/download/111/47/760

[289] Binnemans, K., Jones, P.T., & Blanpain, B. (2024). A Review of the Occurrence and Recovery of Rare Earth Elements from Electronic Waste. Molecules, 29(19), 4624. https://www.mdpi.com/1420-3049/29/19/4624

[290] UNECE. (2025, August 4). Intersection between large-scale digitalization and environmental sustainability: an overview of use and impact of data centres (GEEE-12/2025/INF.2). https://unece.org/sites/default/files/2025-08/GEEE-12.2025.INF_.2%20-%20Sustainability_data.centres.pdf

[291] ITU/UNITAR. (2024). The Global E-waste Monitor 2024. https://ewastemonitor.info/the-global-e-waste-monitor-2024/

[292] ITU. (2024). Press release: A record 62 Mt of e-waste in 2022; only ~1% of REE demand met by recycling. https://www.itu.int/en/mediacentre/Pages/PR-2024-03-20-e-waste-recycling.aspx

[293] European Environment Agency (EEA). (2023). Waste electrical and electronic equipment (WEEE) collection rate (Indicator). https://www.eea.europa.eu/en/european-zero-pollution-dashboards/indicators/waste-electrical-and-electronic-equipment-weee-collection-rate-indicator

[294] European Parliament Research Service (EPRS). (2016). Planned obsolescence: Exploring the issue. https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/581999/EPRS_BRI(2016)581999_EN.pdf

[295] DataCenterDynamics. (2022, March 8). Re-use, refurb, recycle: Circular economy and data center IT assets. https://www.datacenterdynamics.com/en/analysis/re-use-refurb-recycle-circular-economy-thinking-and-data-center-it-assets/

[296] García, M., Smith, L., & Patel, A. (2025). Data centres as a source of flexibility for power systems. Energy Reports, 15, 112–124. https://www.sciencedirect.com/science/article/pii/S2352484725001623

[297] Ember. (2024). EU electricity trends (European Electricity Review 2024). Ember. https://ember-energy.org/latest-insights/european-electricity-review-2024/eu-electricity-trends/

[298] U.S. Department of Energy. (2023). Analysis of hydrogen infrastructure for the feasibility, economics, and sustainability of a fuel cell powered data center (Report No. NREL/TP-5400-1996402). Office of Scientific and Technical Information. https://www.osti.gov/servlets/purl/1996402

[299] National Renewable Energy Laboratory. (2020). Hydrogen and fuel cells for data center applications project meeting: Workshop report (NREL/TP-6A20-75355). National Renewable Energy Laboratory. https://docs.nrel.gov/docs/fy20osti/75355.pdf

[300] Fuel Cell & Hydrogen Energy Association. (2024). How fuel cells help solve the growing data center and AI challenge. https://fchea.org/how-fuel-cells-help-solve-the-growing-data-center-and-ai-challenge/

[301] International Energy Agency. (2025). The path to a new era for nuclear energy (IEA Report). https://iea.blob.core.windows.net/assets/21947d24-cbe3-4fbe-a5b7-5c94de5c60f2/ThePathtoaNewEraforNuclearEnergy.pdf

[302] Nature Editorial. (2025, March 12). Meeting the energy challenge posed by data centres is central to a green future. Nature. https://www.nature.com/articles/d41586-025-00747-3

[303] Li, Y., Chen, Z., & Wang, H. (2024). Data center integrated energy system for sustainability: Generalization, approaches, methods, techniques, and future perspectives. Innovation in Energy, 1(1), 100014. https://doi.org/10.59717/j.xinn-energy.2024.100014

[304] IDTechEx. (2024). Sustainability for data centers 2025–2035: Green technologies, market forecasts, and players.IDTechEx Research. https://www.idtechex.com/en/research-report/sustainability-for-data-centers-2025/1064

[305] Caterpillar Inc. (2024, May 16). Microsoft successfully tests hydrogen fuel cell backup power at data centre. Caterpillar Newsroom. https://www.caterpillar.com/en/news/caterpillarnews/2024/microsoft-hydrogen-fuel-cell-test.html

[306] University of Chicago Climate Research Center. (2025). Reducing data center peak cooling demand and energy costs with underground thermal energy storage. Climate@UChicago. https://climate.uchicago.edu/news/reducing-data-center-peak-cooling-demand-and-energy-costs-with-underground-thermal-energy-storage/

[307] World Nuclear Association. (2024). Nuclear energy and public opinion. World Nuclear Association. https://world-nuclear.org/information-library/current-and-future-generation/nuclear-energy-and-public-opinion

[308] Uptime Institute. (2024). Cooling systems survey 2024: Direct liquid cooling adoption. Uptime Institute. https://datacenter.uptimeinstitute.com/rs/711-RIA-145/images/2024.Cooling.Survey.Report.pdf?version=3&mkt_tok=NzExLVJJQS0xNDUAAAGT7PRR0KuLmMWcCq8tWI21qXB7omLvlzWkBrppTAcUCjbXlkzkaOxnWxRQ-ZovhNilkKVF7w9cDt_um8_igIJ8UIxr8dE0NsyiG0wpj3cL2A

[309] Microsoft. (2025, May 1). Quantifying environmental impacts of datacenter cooling (Nature study). Microsoft News. https://news.microsoft.com/source/features/sustainability/microsoft-quantifies-environmental-impacts-of-datacenter-cooling-from-cradle-to-grave-in-new-nature-study/

[310] European Commission. (n.d.). Digitalisation of the energy system. European Commission. https://energy.ec.europa.eu/topics/eus-energy-system/digitalisation-energy-system_en#:~:text=Due%20for%20publication%20in%20early,side%20flexibility

[311] Patterson, D., Gonzalez, J., Le, Q. V., Liang, C., Munguia, L., Rothchild, D., … Dean, J. (2021). Carbon emissions and large neural network training. arXiv. https://arxiv.org/abs/2104.10350

[312] European Commission. (2025, July 8). EU policy on digitalising and greening the energy system. European Commission. https://digital-strategy.ec.europa.eu/en/policies/eu-policy-digitalisation-energy

[313] Li, P., Yang, J., Islam, M. A., & Ren, S. (2023). Making AI Less "Thirsty": Uncovering and Addressing the Secret Water Footprint of AI Models. arXiv. https://arxiv.org/abs/2304.03271

[314] European Commission. (2024). Commission Delegated Regulation (EU) 2024/1364 establishing a reporting scheme and sustainability rating for data centres. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1364

[315] Eisenband, D. (2024, March 13). 100+ kW per rack in data centers: The evolution and revolution of power density. Ramboll. https://www.ramboll.com/en-us/insights/decarbonise-for-net-zero/100-kw-per-rack-data-centers-evolution-power-density

[316] Bird & Bird. (2024, June 4). Germany: Data centers—PUE limits and heat-reuse obligations (EnEfG §11). Bird & Bird. https://www.twobirds.com/en/insights/2024/germany/rechenzentren-und-abwaerme-ein-ueberblick-ueber-die-gesetzlichen-vorgaben-zur-abwaermenutzung\

[317] Reuters. (2025, August 5). Europe's old power plants to get digital makeover driven by AI boom. Reuters. https://www.reuters.com/sustainability/climate-energy/europes-old-power-plants-get-digital-makeover-driven-by-ai-boom-2025-08-05/

[318] Datacenter Dynamics. (2023, October). Building reuse avoids new embodied carbon. Datacenter Dynamics. https://www.datacenterdynamics.com/en/marketwatch/the-embodied-carbon-challenge-for-truly-net-zero-data-centers/

[319] Joint Research Centre. (2016). Remediated sites and brownfields: Success stories in Europe. European Commission. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC98077/lbna27530enn.pdf

[320] Data Center Frontier. (2022, September). Sustainably meeting high density cooling challenges. Data Center Frontier. https://img.datacenterfrontier.com/files/base/ebm/datacenterfrontier/document/2022/09/1663627616044-dcfspecialreporthighdensitycoolingchallengesv3.pdf

[321] ASHRAE. (2021). Emergence and expansion of liquid cooling in mainstream data centres. ASHRAE. https://www.ashrae.org/file%20library/technical%20resources/bookstore/emergence-and-expansion-of-liquid-cooling-in-mainstream-data-centers_wp.pdf

[322] BD Online. (2024, September 24). New survey finds attitude to urban brownfield regeneration 'overwhelmingly positive'. BD Online. https://www.bdonline.co.uk/news/new-survey-finds-attitude-to-urban-brownfield-regeneration-overwhelmingly-positive/5131774.article

[323] Ford, N. (2025, September 23). Grid investors keen on Europe as energy transition creates openings. Reuters. https://www.reuters.com/business/energy/grid-investors-keen-europe-energy-transition-creates-openings--reeii-2025-09-23/

[324] Fortune. (2025, August 31). AI-center boom repurposes old coal plants. Fortune. https://fortune.com/2025/08/31/ai-data-center-boom-old-coal-plants/

[325] Clean Energy Wire. (2021, March 15). Tesla calls for speedy permits for climate friendly projects in Germany. Clean Energy Wire. https://www.cleanenergywire.org/news/tesla-calls-speedy-permits-climate-friendly-projects-berlin-gigafactory-awaits-approval

[326] Springer. (2022). Reducing Construction Waste Through Modular Construction. In Proceedings of the International Conference on Sustainable Construction. Springer. https://link.springer.com/chapter/10.1007/978-981-19-5256-2_27

[327] Ascon Systems. (2024). Research with digital twins and retrofit: Saving resources. Ascon Systems. https://ascon-systems.de/en/resources/research-with-digital-twins-and-retrofit-saving-resources/

[328] IEA. (2025, April 10). Energy and AI – Analysis - IEA. IEA. https://www.iea.org/reports/energy-and-ai

[329] Bandemer, S., Daßler, B., Rittberger, B., Weiss, M., & Will, K. (2025). Politics of de-risking: how the EU confronts vulnerabilities in critical digital infrastructures. Journal of European Public Policy, 1–29. https://doi.org/10.1080/13501763.2025.2545305

[330] Sun, K., Wang, X., Miao, X., & Zhao, Q. (2024). A review of AI edge devices and lightweight CNN deployment. Neurocomputing, 614, 128791. https://doi.org/10.1016/j.neucom.2024.128791

[331] Takci, M. T., Qadrdan, M., Summers, J., & Gustafsson, J. (2025). Data centres as a source of flexibility for power systems. Energy Reports, 13, 3661–3671. https://doi.org/10.1016/j.egyr.2025.03.020

[332] RMI. (2025, July 17). Fast, flexible solutions for data centers (Yuki Numata, Alexandra Gorin, Laurens Speelman, Lauren Shwisberg, & Chiara Gulli). Rocky Mountain Institute. https://rmi.org/fast-flexible-solutions-for-data-centers/

[333] 3GPP. (2024, May 14). Non-Terrestrial Networks (NTN) Overview. 3GPP. https://www.3gpp.org/technologies/ntn-overview 3GPP

[334] Margaret H. Pinson et al. (2025). Test Plans, Results, and Lessons Learned About Open RAN Integration During the NTIA 5G Challenges, Special Publication NTIA SP-25-578, U.S. Department of Commerce, National Telecommunications and Information Administration, Institute for Telecommunication Sciences, April 2025. https://doi.org/10.70220/xhkcs611

[335] Wilson, D. (2025, July 16). Edge AI Applications: Revolutionizing Industries with AI. Autonomous; Autonomous. https://www.autonomous.ai/ourblog/edge-ai-applications

[336] Knittel, C. R., Senga, J. R., & Wang, S. (2025, July). Flexible Data Centers and the Grid: Lower Costs, Higher Emissions? Working Paper. MIT Center for Energy and Environmental Policy Research. https://ceepr.mit.edu/workingpaper/flexible-data-centers-and-the-grid-lower-costs-higher-emissions/

[337] Lawrence Berkeley National Laboratory. (2025, January 15). Berkeley Lab report evaluates increase in electricity demand from data centers. U.S. Department of Energy. https://newscenter.lbl.gov/2025/01/15/berkeley-lab-report-evaluates-increase-in-electricity-demand-from-data-centers/

[338] Rabobank. (2025, June 24). US data center demand is surging — but where, when, and how much? RaboResearch. https://www.rabobank.com/knowledge/d011483895-us-data-center-demand-is-surging-but-where-when-and-how-much

[339] Urs Hölzle. (2025, August 8). I think it will be "common sense knowledge" in just a few years that AI data centers are grid stabilizers. Linkedin.com. https://www.linkedin.com/posts/urs-h%C3%B6lzle_i-think-it-will-be-common-sense-knowledge-activity-7359503430530330624-jcFH/

[340] Azariah, W., Bimo, F. A., Lin, C.-W., Cheng, R.-G., Nikaein, N., & Jana, R. (2024). A Survey on Open Radio Access Networks: Challenges, Research Directions, and Open Source Approaches. Sensors, 24(3), 1038. https://doi.org/10.3390/s24031038

[341] International Telecommunication Union (2025). Overview of 6G (IMT-2030). https://digitalregulation.org/overview-of-6g-imt-2030/

[342] Regulation (EU) 2023/588 of the European Parliament and of the Council. (2023, March 15). Establishing the Union Secure Connectivity Programme for the period 2023-2027. Official Journal of the European Union. EUR-Lex

[343] Mavrakis, D. (2025, July 1). Open RAN is real, performing and moving forward; there is no way back. RCR Wireless. https://www.rcrwireless.com/20250701/carriers/open-ran-revenue

[344] Edge AI Market Size, Share & Growth | Industry Report, 2030. (n.d.). https://www.grandviewresearch.com/industry-analysis/edge-ai-market-report

[345] Jaycon. (2025, May 15). Top 10 edge AI hardware for 2025. Jaycon. https://www.jaycon.com/top-10-edge-ai-hardware-for-2025/

[346] Belcak, P., Heinrich, G., Diao, S., Fu, Y., Dong, X., Muralidharan, S., Lin, Y. C., & Molchanov, P. (2025, June 2). Small Language Models are the Future of Agentic AI. arXiv. https://arxiv.org/abs/2506.02153

[347] Jensen Huang, CEO Nvidia, Today Magazine. (2025, June 25). The rise of robotics: Nvidia's 2025 prediction. https://www.ceotodaymagazine.com/2025/06/the-robot-decade-nvidia-ceo-declares-ai-driven-machines-will-rule-the-2020s/

[348] Why Europe's critical raw materials strategy has to be international. (2023, March 9). Bruegel | the Brussels-Based Economic Think Tank. https://www.bruegel.org/analysis/why-europes-critical-raw-materials-strategy-has-be-international

[349] Delors Centre. (2024). Meeting the Costs of Resilience: The EU's Critical Raw Materials. https://www.delorscentre.eu/en/publications/eu-critical-raw-materials

[350] European Commission. (2022). CROCODILE: Circular economy of metals – Development of innovative metallurgical systems (Horizon 2020, Deliverable D10.1). https://h2020-crocodile.eu/wp-content/uploads/2022/06/D10.1.pdf

[351] European Commission. (2022). NEMO: Near-zero-waste recycling of low-grade sulphidic mining waste for critical-metal, mineral and construction raw-material production (Horizon 2020). https://h2020-nemo.eu/project-2/nemo-pilots/

[352] European Environment Agency. (2025). Circular material use rate in Europe. Indicator Report. https://www.eea.europa.eu/en/analysis/indicators/circular-material-use-rate-in-europe

[353] Circular Economy. (2025). Environment. https://environment.ec.europa.eu/strategy/circular-economy_en

[354] Institute for European Environmental Policy (IEEP). (2023, October 30). Circularity Gaps of the European Critical Raw Materials Act. https://ieep.eu/publications/circularity-gaps-of-the-european-critical-raw-materials-act/

[355] Schmidt, K. M. (2024, December 9). Supply chain analytics: What is it and why it's important. Stibo Systems. https://www.stibosystems.com/blog/supply-chain-analytics

[356] EIT Digital. (2021). European digital infrastructure and data sovereignty: A policy perspective. https://www.eit.europa.eu/sites/default/files/eit-digital-data-sovereignty-full-report.pdf

[357] The EU's Critical Raw Materials Strategy: Engaging with the World to Achieve Self-Sufficiency. (2024, January 9). Tænketanken Europa. https://thinkeuropa.dk/brief/2024-09-the-eus-critical-raw-materials-strategy-engaging-with-the-world-to-achieve-self

[358] Clean Tech Lithium. (2022, August 19). Direct Lithium Extraction. Ctlithium.com. https://ctlithium.com/about/direct-lithium-extraction/

[359] Katja Götze, Hedrich, S., Braeuer, A. S., & Haseneder, R. (2024). Process Optimization of an In-Situ Bioleaching Section with Associated Membrane Filtration in a Field Test Laboratory. Minerals, 14(3), 308–308. https://doi.org/10.3390/min14030308

[360] Cordis, C. (2024, January 8). A sustainable ecosystem for the innovative resource recovery and complex ore extraction. CORDIS | European Commission. https://cordis.europa.eu/project/id/101138432

[361] SYSTEMIQ. (2024). A critical raw material supply-side innovation roadmap. SYSTEMIQ. https://www.systemiq.earth/wp-content/uploads/2024/12/2024-12-10-EU-CRM-Innovation-Roadmap-vFinal-1.0.pdf

[362] Fraunhofer Institute for Ceramic Technologies and Systems IKTS. (2025, January 15). On the way to a cost-effective sodium battery. https://www.ikts.fraunhofer.de/en/press_media/press_releases/2025-1-15_n_on-the-way-to-sodium-battery.html

[363] Merchant, A., Batzner, S., Schoenholz, S. S., Aykol, M., Cheon, G., & Cubuk, E. D. (2023). Scaling deep learning for materials discovery. Nature, 624(7990), 80–85. https://doi.org/10.1038/s41586-023-06735-9

[364] Critical Raw Materials Act. 2024. Internal Market, Industry, Entrepreneurship and SMEs. https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials/critical-raw-materials-act_en

[365] UCL Bartlett Faculty of the Built Environment. (2025, May 8). Digital sovereignty for people and the planet: How to get there? University College London. https://www.ucl.ac.uk/bartlett/events/2025/may/digital-sovereignty-people-and-planet-how-get-there

[366] Institute for European Environmental Policy. (2023). Circularity and the European Critical Raw Materials Act. https://ieep.eu/wp-content/uploads/2023/10/Circularity-and-the-European-Critical-Raw-Materials-Act-IEEP-2023.pdf

[367] Potting, J., Hekkert, M., Worrell, E, Hanemaaijer, E. (2017). Circular Economy: Measuring Innovation in the Product Chain. https://www.pbl.nl/uploads/default/downloads/pbl-2016-circular-economy-measuring-innovation-in-product-chains-2544.pdf

[368] International Resource Panel. (2017). Assessing global resource use: A systems approach to resource efficiency and pollution reduction. https://www.resourcepanel.org/sites/default/files/documents/document/media/assessing_global_resource_use_amended_130318.pdf

[369] Formentini, G., Prioli, J. PJ., Ko, J., Hapuwatte, B., Ferrero, V., Badurdeen, F., Rickli, J. L., & Ramanujan, D. (2025). A review of disassembly systems for circular product design. Journal of Cleaner Production, 506, 145459. https://doi.org/10.1016/j.jclepro.2025.145459

[370] Antikainen, R., Baudry, R., Gössnitzer, A., Kaisa, T., Karppinen, M., Kishna, M., Montevecchi, F., Müller, F., Pinet, C., & Uggla, R. (2021). European Network of the Heads of Environment Protection Agencies (EPA Network) -Interest Group on Green and Circular Economy CIRCULAR BUSINESS MODELS: PRODUCT-SERVICE SYSTEMS ON THE WAY TO A CIRCULAR ECONOMY. https://epanet.eea.europa.eu/reports-letters/reports-and-letters/circular_business_models_interest-group-green-and-circular-economy.pdf

[371] Corrado, C., et al. (2022). Measuring data as an asset: Framework, methods and preliminary estimates (OECD Economics Department Working Papers No. 1731). OECD Publishing. https://doi.org/10.1787/b840fb01-en

[372] Synergy Research Group. (2022). European Cloud Providers' Local Market Share Now Holds Steady at 15%. https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15

[373] Big Data Value Association (BDVA). (2023). Vision paper: European Federation of Data Innovation Spaces (i-Spaces).BDVA / EUHubs4Data. https://bdva.eu/news/vision-paper-european-federation-of-data-innovation-spaces-i-spaces/

[374] European Commission. (2025). State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future(COM(2025) 290 final). Publications Office of the European Union. https://digital-strategy.ec.europa.eu/en/library/state-digital-decade-2025-report

[375] Big Data Value Association. (n.d.). Big Data Value Association – Accelerating data-driven innovation in Europe. Retrieved September 30, 2025, from https://bdva.eu

[376] European Parliament. (2025). Report on European technological sovereignty and digital autonomy. Committee on Industry, Research and Energy. https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.html

[377] Borrell, J. (2024, October 12). Defence technologies – Time to think big again. EEAS. https://www.eeas.europa.eu/eeas/defence-technologies-time-think-big-again_en

[378] European Union Agency for Cybersecurity (ENISA). (2024). Cybersecurity Threats Fast Forward 2030. https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

[379] Bondar, K. (2025). Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare. Center for Strategic & International Studies (CSIS). https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare

[380] Staff, T. & AFP. (2025, April 20). Israel's new unmanned bulldozers "changing the paradigm" of war in Gaza. The Times of Israel. https://www.timesofisrael.com/israels-new-unmanned-bulldozers-changing-the-paradigm-of-war-in-gaza/

[381] ENISA. (2024). Foresight Cybersecurity Threats for 2030 Update 2024. https://www.enisa.europa.eu/sites/default/files/2024-11/Foresight%20Cybersecurity%20Threats%20For%202030%20Update%202024_0.pdf

[382] EUSPA. (2024). EUSPA EO and GNSS market report (Issue 2, 2024). European Union Agency for the Space Programme. https://www.euspa.europa.eu/sites/default/files/2024-03/euspa_market_report_2024.pdf

[383] Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means. Research Policy, 52(6), 104765. https://doi.org/10.1016/j.respol.2023.104765

[384] Teal Communications Staff. (2023, November 2). The rise of autonomous robots in warfare: A look into the future of connected combat. Cellular IoT Connectivity | True eSIM From TEAL. https://tealcom.io/post/the-rise-of-autonomous-robots-in-warfare-emerging-examples-and-impacts/

[385] Grand View Research. (2025, May 22). Europe Military Robots Market Size & Outlook, 2030. Grand View Horizon. https://www.grandviewresearch.com/horizon/outlook/military-robots-market/europe

[386] Gordan, M., Djibrilla Amadou Kountche, McCrum, D., Schauer, S., König, S., Delannoy, S., Connolly, L., Mircea Iacob, Nicola Gregorio Durante, Yash Shekhawat, Carrasco, C., Takis Katsoulakos, & Carroll, P. (2024). Protecting critical infrastructure against cascading effects: The PRECINCT approach. Resilient Cities and Structures, 3(3), 1–19. https://doi.org/10.1016/j.rcns.2024.04.001

[387] Communications Security Establishment Canada. (2024). National Cyber Threat Assessment 2025-2026. Government of Canada. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026

[388] Ibraheem, I. O., & Bello-Ahmed, L. (2025). Green tech, safe networks: the role of cybersecurity in combating climate change. Discover Internet of Things, 5(1). https://doi.org/10.1007/s43926-025-00125-5

[389] ENISA. (2024). Skills Shortage and Unpatched Systems Soar to High-Ranking 2030 Cyber Threats. https://www.enisa.europa.eu/news/skills-shortage-and-unpatched-systems-soar-to-high-ranking-2030-cyber-threats

[390] ESPI. (2025, January 28). An initial perspective on a European space strategy 2040: From vision towards implementation. European Space Policy Institute. https://www.espi.or.at/wp-content/uploads/2025/01/ESPI-Initial-Perspective-on-a-European-Space-Strategy-2040-Jan-2025.pdf

[391] Wohrer, P. (2025, March 17). The European space model: Renewing ambition in a changing strategic landscape. IFRI. https://www.ifri.org/sites/default/files/2025-04/ifri_wohrer_european_space_model_2025.pdf

[392] Hader, M., & Kirstetter, E. (2025, June 2). A revolution in space? How the low Earth orbit economy can create radical solutions and innovative opportunities for traditional industries. Roland Berger. https://www.rolandberger.com/en/Insights/Publications/A-revolution-in-space.html

[393] Hader, M., Kirstetter, E., Hader, M., & Kirstetter, E. (2025, June 2). A revolution in space? Roland Berger. https://www.rolandberger.com/en/Insights/Publications/A-revolution-in-space.html

[394] Etzioni, A., & Etzioni, O. (2017, April 28). Pros and cons of autonomous weapons systems. Military Review, May–June 2017. Social Science Research Network. https://ssrn.com/abstract=2960301

[395] Benson, E., Bergmann, M. & Steinberg, F. (2025, 5. Mai). The Transatlantic Tech Clash: Will Europe "De-Risk" from the United States? Center For Strategic And International Studies. https://www.csis.org/analysis/transatlantic-tech-clash-will-europe-de-risk-united-states

[396] Thompson, P. (2024, March 28). Palmer Luckey says Anduril is working on AI weapons that "give us the ability to swiftly win any war." Business Insider. https://www.businessinsider.com/palmer-luckey-anduril-defense-startup-ai-weapons-war-2024-3

[397] CyberCX. (2023). Ciaran Martin: Resilience Key to Cyber Defence. https://cybercx.com.au/resource/ciaran-martin-resilience-key-to-cyber-defence/

[398] Forzieri, G., Bianchi, A., Silva, F. B. E., Marin Herrera, M. A., Leblois, A., Lavalle, C., Aerts, J. C. J. H., & Feyen, L. (2018). Escalating impacts of climate extremes on critical infrastructures in Europe. Global Environmental Change, 48, 97–107. https://doi.org/10.1016/j.gloenvcha.2017.11.007

[399] ComputerWeekly. (2025). Ciaran Martin: AI Might Disturb Attacker-Defender Security Balance. https://www.computerweekly.com/news/366626443/Ciaran-Martin-AI-might-disturb-attacker-defender-security-balance

[400] Eurocontrol. (2024). ATM: Navigating the Challenging Cybersecurity Landscape. https://www.eurocontrol.int/article/atm-navigating-challenging-cybersecurity-landscape

[401] Cybersecurity and Infrastructure Security Agency (CISA). (2025). International Strategic Plan 2025–2026. https://www.cisa.gov/2025-2026-cisa-international-strategic-plan

[402] https://www.csis.org/analysis/transatlantic-tech-clash-will-europe-de-risk-united-states

[403] Hader, M., & Hader, M. (2023, October 18). Space-enabled Germany. Roland Berger. https://www.rolandberger.com/en/Insights/Publications/Space-enabled-Germany.html

[404] Hillmann, S., & Wachter, M. (2022, January 27). New Space is becoming increasingly important for German industry. BDI. https://english.bdi.eu/article/news/new-space-is-becoming-increasingly-important-for-german-industry

[405] European Commission. (2021). Europe's Digital Decade: digital targets for 2030. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

[406] https://ailiteracyframework.org/wp-content/uploads/2025/05/AILitFramework_ReviewDraft.pdf

[407] The Entrepreneurial University - TUM. (2025, September 26). Tum.de; TUM. https://tum.de

[408] KPMG Finland. (2025, January 2). EU talent attraction: Addressing the skilled worker shortage. https://kpmg.com/fi/en/insights/tax-and-legal/eu-talent-attraction-addressing-the-skilled-worker-shortage.html

[409] European Commission. (2022). DESI | Shaping Europe's digital future. Digital-Strategy.ec.europa.eu. https://digital-strategy.ec.europa.eu/en/policies/desi

[410] Balland, P.-A., Di Girolamo, V., Benoit, F., Ravet, J., & Hobza, A. (n.d.). Divided We Fall Behind Why a fragmented EU cannot compete in complex technologies. https://doi.org/10.2777/8548441

[411] Digital by default: A guide to transforming government. (n.d.). https://www.mckinsey.com/~/media/mckinsey/industries/public%20and%20social%20sector/our%20insights/transforming%20government%20through%20digitization/digital-by-default-a-guide-to-transforming-government-final.pdf

[412] EdTechReview Editorial Team. (2023, June 6). What is digital literacy, its importance, and challenges? EdTechReview. https://www.edtechreview.in/trends-insights/insights/what-is-digital-literacy-its-importance-and-challenges/

[413] European Education Area. (2024, November 13). Lagging digital literacy among 14-year-olds across the EU, study finds. European Education Area. https://education.ec.europa.eu/news/lagging-digital-literacy-among-14-year-olds-across-the-eu-study-finds

[414] Wire. (2025, August 12). The State of Digital Sovereignty in Europe 2025 | Wire Survey & Insights. Wire.com. https://wire.com/en/blog/state-digital-sovereignty-europe

[415] European Commission. (2025, June 3). Divided we fall behind: Why a fragmented EU cannot compete in complex technologies. Research and Innovation. https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/divided-we-fall-behind-why-fragmented-eu-cannot-compete-complex-technologies_en

[416] Bianchini, N., & Ancona, L. (2023). Artificial Intelligence: Europe must start dreaming again. https://server.www.robert-schuman.eu/storage/en/doc/questions-d-europe/qe-728-en.pdf

[417] European Parliament. (2021). Digital skills and the future of work (EPRS Study No. 697184). https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697184/EPRS_STU(2021)697184_EN.pdf

[418] European innovation scoreboard 2023. (2024). Research-And-Innovation.ec.europa.eu. https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/european-innovation-scoreboard-2023_en

[419] OECD. (2021). OECD Studies on SMEs and Entrepreneurship The Digital Transformation of SMEs. https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/02/the-digital-transformation-of-smes_ec3163f5/bdb9256a-en.pdf

[420] Deutscher Startup Monitor Den Blick nach vorne 2 0 2 4. (n.d.). https://startupverband.de/fileadmin/startupverband/mediaarchiv/research/dsm/Deutscher_Startup_Monitor_2024.pdf

[421] European Commission. (2024, May 21). Pact on Migration and Asylum. European Commission. https://home-affairs.ec.europa.eu/policies/migration-and-asylum/pact-migration-and-asylum_en

[422] Kosyakova, Y., Olbrich, L., Gallegos Torres, K., Hammer, L., Koch, T., & Wagner, S. (2025). Deutschland als Zwischenstation? Rückkehr- und Weiterwanderungsabsichten von Eingewanderten im Lichte neuer Daten des International Mobility Panel of Migrants in Germany (IMPa). IAB-Forschungsbericht 15/2025. Institut für Arbeitsmarkt- und Berufsforschung (IAB). https://doi.org/10.48720/IAB.FB.2515

[423] OECD. (2024). International Migration Outlook 2024. OECD. https://www.oecd.org/en/publications/2024/11/international-migration-outlook-2024_c6f3e803.html

[424] EURES Report on labour shortages and surpluses 2023. (2023). https://www.ela.europa.eu/sites/default/files/2024-05/EURES-Shortages_Report-V8.pdf

[425] Benini, F. (2024). Toward a shared, sovereign and collaborative internet. Commons Network. https://www.commonsnetwork.org/wp-content/uploads/2024/10/Digital-Commons-Event-Report-eng.pdf

[426] Warso, Z. (2025, June 10). Europe Talks Digital Sovereignty. Open Future. https://openfuture.eu/blog/europe-talks-digital-sovereignty/

[427] Frion, L. (2022). Digital commons as alternative governance and value systems. Sciences Po. https://www.sciencespo.fr/public/chaire-numerique/wp-content/uploads/2023/06/15-juin-DIGITAL-COMMONS-policy-brief-Louise-Frion-1.pdf

[428] Bloemen, S. (2025). Digital Commons governance models toward digital sovereignty. NGI Commons. https://commons.ngi.eu/2025/02/10/webinar-series-report-digital-commons-towards-digital-sovereignty-in-europe/

[429] European Commission. (n.d.). European Open Science Cloud (EOSC). Retrieved September 27, 2025, https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/our-digital-future/open-science/european-open-science-cloud-eosc_en

[430] NGI Commons. (n.d.). About. In NGI Commons. Retrieved September 21, 2025, from https://commons.ngi.eu/about/

[431] EPI Company. (n.d.). Home. In EPI Company. Retrieved September 27, 2025, from https://epicompany.eu

[432] Jussen, I., Möller, F., Schweihoff, J., Gieß, A., Giussani, G., & Otto, B. (2024). Issues in inter-organizational data sharing: Findings from practice and research challenges. Data & Knowledge Engineering, 150, 102280. https://doi.org/10.1016/j.datak.2024.102280

[433] Gates, N., Tridgell, J., Torraco, R. M., Schwäbe, C., Reda, F., Hummler, A., Streinz, T., Nummelin Carlberg, A., & Blind, K. (2025). Funding Europe's open digital infrastructure: A study on the economic, legal, and political feasibility of an EU sovereign tech fund (EU-STF) (OFE Publ. No. 9789090405315). OpenForum Europe. https://doi.org/10.24406/publica-4949

[434] Baur, A. (2025). European ambitions captured by American clouds: digital sovereignty through Gaia-X? Information Communication & Society, 1–18. https://doi.org/10.1080/1369118x.2025.2516545

[435] Kouroubali, A., & Katehakis, D. G. (2019). The new European interoperability framework as a facilitator of digital transformation for citizen empowerment. Journal of Biomedical Informatics, 94, 103166. https://doi.org/10.1016/j.jbi.2019.103166

[436] Musiani, F. (2025, June 18). Gaia-X: the bid for a sovereign European cloud. Polytechnique Insights. Retrieved September 27, 2025, https://www.polytechnique-insights.com/en/columns/digital/gaia-x-the-bid-for-a-sovereign-european-cloud/

[437] ETSI. (2024). Standards in support of Europe's digital infrastructure needs (ETSI White Paper No. WP-63). https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP-63-Standards_in_support_of_Europes_Digital_Infrastructure_Needs_.pdf

[438] Bria, F. (2023, December 10). Open, sovereign, independent AI: Europe's greatest challenge? Medium. https://medium.com/%40francescabria/open-sovereign-independent-ai-europes-greatest-challenge-6c8a899041ec

[439] Poteralska, M., & Perek-Bialas, J. (2024). The importance of employee skills on a technologically transforming labor market: An empirical analysis from the perspective of employers. Zarządzanie Zasobami Ludzkimi, 157(2), 30-54. https://doi.org/10.5604/01.3001.0054.6535

[440] Mercer, & Oliver Wyman. (2018, June). Delivering the workforce for the future: Open-source talent. Oliver Wyman. https://www.oliverwyman.de/content/dam/oliver-wyman/v2/publications/2018/june/Open-Source-Talent.pdf

[441] Hazan, E., Madgavkar, A., Chui, M., Smit, S., Maor, D., Dandona, G. S., & Huyghues-Despointes, R. (2024, May 21). A new future of work: The race to deploy AI and raise skills in Europe and beyond. McKinsey Global Institute. https://www.mckinsey.com/mgi/our-research/a-new-future-of-work-the-race-to-deploy-ai

[442] Petry, J. (2025, September 17). VC Interviews at CDTM with Jana Petry from UVC Partners.

[443] TestGorilla. (n.d.). The state of skills-based hiring 2025. Retrieved September 27, 2025, https://www.testgorilla.com/skills-based-hiring/state-of-skills-based-hiring-2025

[444] Górka, J. (Ed.). (2016). Transforming payment systems in Europe. Palgrave Macmillan. https://doi.org/10.1057/9781137541215

[445] Gronholt-Pedersen, J., & Strupczewski, J. (2025, September 19). EU ministers seek agreement on digital euro to be independent of Visa and Mastercard. Reuters. https://www.reuters.com/business/finance/eu-ministers-seek-agreement-digital-euro-be-independent-visa-mastercard-2025-09-19/

[446] Cipollone, P. (2025, February 28). The role of the digital euro in digital payments and finance. European Central Bank. https://www.ecb.europa.eu/press/inter/date/2025/html/ecb.in250228~7c25c90e4d.en.html

[447] Cerutti, E. M., Firat, M., & Perez-Saiz, H. (2025). Estimating the impact of digital money on cross-border flows: Scenario analysis covering the intensive margin (Fintech Notes No. 2025/002). International Monetary Fund. https://doi.org/10.5089/9798229000611.063

[448] Rastogi, S., Panse, C., Sharma, A., & Bhimavarapu, V. M. (2021). Unified Payment Interface (UPI): A digital innovation and its impact on financial inclusion and economic development. Universal Journal of Accounting and Finance, 9(3), 518–530. https://doi.org/10.13189/ujaf.2021.090326

[449] Cipollone, P. (2024, September 27). Monetary sovereignty in the digital age: The case for a digital euro [Keynote speech]. European Central Bank. https://www.ecb.europa.eu/press/key/date/2024/html/ecb.sp240927~11ed8493a4.en.html

[450] Polinati, A. K. (2025). Hybrid cloud security: Balancing performance, cost, and compliance in multi-cloud deployments. arXiv. https://arxiv.org/abs/2506.00426

[451] Feretzakis, G., & Verykios, V. S. (2024). Trustworthy AI: Securing sensitive data in large language models. AI, 5(4), 2773–2800. https://doi.org/10.3390/ai5040134

[452] Khan, A. R. (2024). Dynamic Load Balancing in Cloud Computing: Optimized RL-Based Clustering with Multi-Objective Optimized Task Scheduling. Processes, 12(3), 519. https://doi.org/10.3390/pr12030519

[453] Dong, S., Tang, J., Abbas, K., Hou, R., Kamruzzaman, J., Rutkowski, L., & Buyya, R. (2024). Task offloading strategies for mobile edge computing: A survey. Computer Networks, 110791. https://doi.org/10.1016/j.comnet.2024.110791

[454] Baur, D., Seybold, D., Griesinger, F., Masata, H., & Domaschka, J. (2018). A Provider-Agnostic Approach to Multi-cloud Orchestration Using a Constraint Language. Cluster Computing and the Grid (CCGRID), IEEE/ACM International Symposium, 2018, 173–182. https://doi.org/10.1109/ccgrid.2018.00032

[455] Eurostat. (2024, December 5). Large businesses make up only 0.2% of EU enterprises. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20241205-1

[456] International Data Corporation. (2024, September 10). Global spending on edge computing to reach $228 billion in 2024, according to IDC's Worldwide Edge Spending Guide. https://my.idc.com/getdoc.jsp?containerId=prUS52587424

[457] Intelligence, M. (2025, July 6). Hybrid Cloud Market - Share, size, growth & Forecast | 2025-2030. Mordor Intelligence. https://www.mordorintelligence.com/industry-reports/hybrid-cloud-market

[458] Flexera. (2024, March 12). Flexera 2024 State of the Cloud: Managing Cloud Spending is the Top Challenge of Cloud Computing, while AI, FinOps, Security and Sustainability Demand Attention. https://www.flexera.com/about-us/press-center/flexera-2024-state-of-the-cloud-managing-spending-top-challenge

[459] AI Workload Strategies 2025. (2025). S&P. https://www.telehouse.net/wp-content/uploads/2025/04/Telehouse_AI_Workload_Strategies_2025.pdf

[460] Akash Network. (n.d.). Decentralized Compute Marketplace. https://akash.network/

[461] ZEDEDA. (n.d.). Solutions. In ZEDEDA. Retrieved September 27, 2025, from https://zededa.com/solutions/

[462] RAFAY. (n.d.). Why Rafay?. In Rafay. Retrieved September 25, 2025, from https://rafay.co/why-rafay/

[463] Vlaskamp, M. C. (2024). Looking for resource sovereignty in a fragmenting global order: The EU's response to critical raw materials challenges. In O. Costa, E. Soler i Lecha, & M. C. Vlaskamp (Eds.), EU Foreign Policy in a Fragmenting International Order (pp. 147–175). Springer.

[464] Li, P., Chen, Y., & Guo, X. (2025). Digital transformation and supply chain resilience. International Review of Economics & Finance, 99. https://doi.org/10.1016/j.iref.2025.104033

[465] European Parliament. (2025, June 11). Report on European technological sovereignty and digital infrastructure (A10-0107/2025). https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.html

[466] Zhao, Y., Chen, G., & Liu, J. (2025). Polymer data challenges in the AI era: Bridging gaps for next-generation energy materials [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2505.13494

[467] Li, Y., Smith, J., Wang, X., & Chen, R. (2022). Reproducible and attributable materials science workflows. Materials Science and Engineering: R: Reports, 145, 100624. https://doi.org/10.1016/j.mser.2022.100624

[468] Himanen, L., Geurts, A., Foster, A. S., & Rinke, P. (2019). Data-driven materials science: Status, challenges, and perspectives. Advanced Science, 6(24), 1900808. https://doi.org/10.1002/advs.201900808

[469] Activate. (2025). Newfound Materials. In Activate. Retrieved September 26, 2025, https://www.activate.org/newfound-materials

[470] Mariev, O. (2025). Interplay of Chinese rare earth elements supply and European renewable energy sectors. Renewable Energy, 2024, 121986. https://doi.org/10.1016/j.renene.2024.121986

[471] Emergen Research. (2025). AI-Driven Materials Discovery Platforms Market Size, Share, Trend Analysis by 2033. In Emergen Research. Retrieved September 26, 2025, https://www.emergenresearch.com/industry-report/ai-driven-materials-discovery-platforms-market

[472] Mordor Intelligence. (2025, August 8). Material Informatics Market Size, Share & 2030 Growth Trends Report. Global Material Informatics Market. Retrieved September 26, 2025, https://www.mordorintelligence.com/industry-reports/material-informatics-market

[473] Research and Markets. (2025, March). Material Informatics Market Size, Share & Forecast to 2030. https://www.researchandmarkets.com/report/material-informatics?srsltid=AfmBOorqdRTUR5hBthF44oDXNqfNwM2fQjkbXuQvlhnUCpzfO5Oa8Dxd

[474] Grand View Research. (2023). Material Informatics Market (2024 - 2030) - Size, Share & Trends Analysis Report By Material Type (Elements, Chemicals), By Technology (Machine Learning, Deep Tensor), By End-use, By Region, And Segment Forecasts. In Grand View Research. Retrieved September 26, 2025, https://www.grandviewresearch.com/industry-analysis/material-informatics-market-report

[475] EU Space Strategy for Security and Defence. (n.d.). Defence Industry and Space. https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en

[476] Cellerino, C. (2023). EU Space Policy and Strategic Autonomy: Tackling legal complexities in the enhancement of the 'Security and Defence dimension of the Union in Space.' European Papers. https://doi.org/10.15166/2499-8249/669

[477] ESA Space Environment Report 2024. (2024, July 19). https://www.esa.int/Space_Safety/Space_Debris/ESA_Space_Environment_Report_2024

[478] Ribeiro, A. (2025, April 2). EU analysis highlights space capabilities, lists scenarios for space security by 2050. Industrial Cyber. https://industrialcyber.co/reports/eu-analysis-highlights-space-capabilities-lists-scenarios-for-space-security-by-2050/

[479] NASA. (2023). 65 Years Ago: Sputnik Ushers in the Space Age. https://www.nasa.gov/history/65-years-ago-sputnik-ushers-in-the-space-age/

[480] Goldman Sachs. (2025, March 5). The global satellite market is forecast to become seven times bigger. Goldmansachs.com. https://www.goldmansachs.com/insights/articles/the-global-satellite-market-is-forecast-to-become-seven-times-bigger

[481] NanoAvionics. (2025). What are satellites used for? https://nanoavionics.com/blog/what-are-satellites-used-for/

[482] ESA Space Environment Report 2025. (2025, April 1). https://www.esa.int/Space_Safety/Space_Debris/ESA_Space_Environment_Report_2025

[483] Sternula. (2025). Space Debris and Kessler Syndrome: Mitigating the Risks of Spaceflight. https://www.sternula.com/space-debris-and-kessler-syndrome-mitigating-the-risks-of-spaceflight/

[484] JAXA. (2022). REMOVAL of SPACEPACE DEBRIS | CRD2. https://www.kenkai.jaxa.jp/eng/crd2/about/

[485] Klinkrad, H., & Johnson, N. L. (2009). Space debris environment remediation concepts (Paper No. 88, in Proceedings of the 5th European Conference on Space Debris). ESA. https://conference.sdo.esoc.esa.int/proceedings/sdc5/paper/88/SDC5-paper88.pdf

[486] Massucci-Templier, C. (2024, September 10). Space Security and Defense: A New Era of Strategic Priorities. Constellations. https://www.kratosspace.com/constellations/articles/space-security-and-defense-a-new-era-of-strategic-priorities

[487] EU Space and Defence Industry for a more Innovative Europe. (n.d.). Defence Industry and Space. https://defence-industry-space.ec.europa.eu/innovative-europe_en

[488] Wall, R. (2025, January 31). EU earmarks $1.1B for 2025 defense R&D collaboration. Aviation Week Network. https://aviationweek.com/defense/budget-policy-operations/eu-earmarks-11b-2025-defense-rd-collaboration

[489] The Space Review: Through a glass, darkly: Chinese, American, and Russian anti-satellite testing in space (page 2). (n.d.). https://www.thespacereview.com/article/2473/2

[490] Bingen, K. A., Johnson, K., Young, M., & Raymond, J. W. (2023). SPACE THREAT ASSESSMENT 2023. In CSIS. https://aerospace.csis.org/wp-content/uploads/2023/04/230414_Bingen_SpaceThreatAssessment_2023_UPDATED-min.pdf

[491] COSMIC | Astroscale's UK-Led Robotic Debris Removal Mission. (n.d.). Astroscale. https://www.astroscale.com/en/missions/cosmic

[492] ClearSpace-1 MISSION. (n.d.). https://clearspace.today/missions/clearspace-1

[493] Turion Space | Propulsion. (n.d.). https://turionspace.com/propulsion

[494] Space. (2025, July 14). GMV. https://www.gmv.com/en-es/sectors/space

[495] Kall Morris Inc. (n.d.). Kall Morris Incorporated. https://www.kallmorris.com/

[496] Orbital Lasers. (n.d.). Orbital Lasers. https://www.orbitallasers.com/

[497] Joint-forces.com. (2021, November 20). Raytheon, Lockheed Martin and Northrop Grumman GPI contracts. Joint Forces News. https://www.joint-forces.com/space-and-aero/48438-raytheon-lockheed-martin-and-northrop-grumman-gpi-contracts

[498] Forging the space armory. (n.d.). Dark. https://www.dark-space.co/mission-forging-the-space-armory

[499] GuardianSat - Space Domain Defense. (n.d.). GuardianSat. https://gsat.space/

[500] Anduril and Impulse Space expand partnership to conduct RPO Mission demonstration in GEO. (n.d.). Anduril. https://www.anduril.com/article/anduril-and-impulse-space-expand-partnership-to-conduct-rpo-mission-demonstration-in-geo/

[501] European Union. (2023, December 6). Digital literacy in the EU: An overview. https://data.europa.eu/en/publications/datastories/digital-literacy-eu-overview

[502] Joint Research Centre. (2025, March 5). How to reach the EU target of 80% of adults with basic digital skills by 2030? European Commission. https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/how-reach-eu-target-80-adults-basic-digital-skills-2030-2025-03-05_en

[503] Mimecast. (2025). The State of Human Risk 2025. https://www.mimecast.com/resources/ebooks/state-of-human-risk-2025/

[504] Ugbebor, F. (2024). Employee cybersecurity awareness training programs customized for SME contexts to reduce human-error-related security incidents. Journal of Knowledge and Learning Science & Technology, 1(1), 1–15. https://jklst.org/index.php/home/article/view/276

[505] GlobalNewswire. (2025, July 31). Corporate Training Market Outlook Report 2025-2030: Digital Learning Platforms to Dominate Corporate Training with 93% Adoption by 2025. https://finance.yahoo.com/news/corporate-training-market-outlook-report-080500710.html?guccounter=1

[506] CognitiveMarketResearch. (2025, July). Europe Corporate Training Market Report 2025. https://wwwcognitivemarketresearch.com/regional-analysis/europe-corporate-training-market-report

[507] Mastercard. (2025, May 27). Cyber fraud threatens small businesses in Europe – One in four small businesses in Europe at risk of closure due to cyber fraud.

https://www.mastercard.com/news/europe/en/newsroom/press-releases/en/2025/cyber-fraud-threatens-small-businesses-in-europe-one-in-four-small-businesses-in-europe-at-risk-of-closure-due-to-cyber-fraud/

[508] Regnier, L. (n.d.). 48 % of SMEs admit they do not provide cyber security training. Startups Magazine. https://startupsmagazine.co.uk/article-48-smes-admit-they-do-not-provide-cyber-security-training

[509] European Commission. (n.d.-b). NIS2 directive: Securing network and information systems. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[510] Official NIS2 Website. (2025). New Organizational Requirements. https://nis2directive.eu/nis2-requirements/

[511] ICO - Information Commissioner's Office. (2023). Errors: Learning from the mistakes of others – A retrospective review. https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/learning-from-the-mistakes-of-others-a-retrospective-review/errors/

[512] European Digital SME Skill Alliance. (2021, August 12). Digital Skills for SMEs: Challenges and Opportunities. https://www.digitalsme.eu/digital-skills-for-smes-challenges-and-opportunities/

[513] Yuan, X. (2022). Evidence of the spacing effect and influences on perceptions of learning and science curricula. Cureus, 14(1), 1–10. https://doi.org/10.7759/cureus.21201

[514] BuildEmpire. (2025). Gamification statistics you need for 2026. In BuildEmpire. https://buildempire.co.uk/gamification-statistics/

[515] Cognitive Market Research. (2025). Europe corporate training industry report. https://www.cognitivemarketresearch.com/regional-analysis/europe-corporate-training-market-report

[516] Infosecurityeurope. (2024, February 1). NIS 2 is Coming: What Does It Mean for EU and Non-EU Organisations?. https://www.infosecurityeurope.com/en-gb/blog/regulation-and-policy/nis2-directive-compliance.html

[517] Chaudhary, S., Vasileios Gkioulos, & Goodman, D. W. (2023). Cybersecurity Awareness for Small and Medium-Sized Enterprises (SMEs): Availability and Scope of Free and Inexpensive Awareness Resources. Lecture Notes in Computer Science, 97–115. https://doi.org/10.1007/978-3-031-25460-4_6

[518] Pluralsight. (2019). Pluralsight - Unlimited Online Developer, IT, and Cyber Security Training. Pluralsight.com. https://www.pluralsight.com/

[519] Skillsoft | Online Courses and Training | Free Access. (n.d.). Skillsoft. https://www.skillsoft.com/

[520] LinkedIn. (2025). LinkedIn Learning: Online Courses for Creative, Technology, Business Skills. Linkedin. https://www.linkedin.com/learning/

[521] Coursera. (2025). Coursera | Online Courses & Credentials by Top Educators. Join for Free. Coursera; Coursera. https://www.coursera.org/

[522] KnowBe4. (2018). Security Awareness Training . Knowbe4.com. https://www.knowbe4.com/

[523] Security awareness and human risk management. (2022, February 2). SoSafe. https://sosafe-awareness.com/?_gl=1

[524] The Hoxhunt Human Risk Management Platform. (2024). Hoxhunt.com. https://hoxhunt.com/

[525] Duolingo. (2025). Learn a Language for Free. Duolingo. https://www.duolingo.com/

[526] Kahoot. (2024). Kahoot! Kahoot! https://kahoot.com/

[527] Katsinis, A., Lagüera-González, J., Di Bella, L., Odenthal, L., Hell, M., & Lozar, B. (2024). Annual report on European SMEs 2023/2024. Publications Office of the European Union. https://doi.org/10.2826/355464

[528] Madgavkar, A., Piccitto, M., White, O., Ramírez, M. J., Mischke, J., & Chockalingam, K. (2024, May 2). A microscope on small businesses: Spotting opportunities to boost productivity. McKinsey Global Institute. https://www.mckinsey.com/mgi/our-research/a-microscope-on-small-businesses-spotting-opportunities-to-boost-productivity

[529] Guide to Safe Payments. (2024). Payment Card Industry Security Standards Council. https://listings.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf

[530] Kappel, R. (2025, May 8). How much does PCI DSS compliance cost in 2025? Centraleyes. https://www.centraleyes.com/pci-dss-compliance-cost/

[531] Wise. (2024, January). Hidden fees. In Wise. https://wise.com/campaign/hidden-fees-eu

[532] Mastercard. (2023). Borderless Payments Report 2023: Making Money Go Further. https://www.mastercard.com/global/en/business/payments/mastercard-move/borderless-payments-report.html

[533] Clearly Payments. (n.d.). Key differences of payments for small businesses vs. enterprises. https://www.clearlypayments.com/blog/key-differences-of-payments-for-small-businesses-vs-enterprises/

[534] IntelliPay. (2025, August 13). Payment processing costs surge for small businesses. IntelliPay. https://intellipay.com/payment-processing-costs-surge-for-small-businesses/

[535] JPMorgan. (2023). Cross-border payment modernization. Payments Unbound, Volume 3. https://www.jpmorgan.com/payments/payments-unbound/volume-3/cross-border-payment-modernization

[536] Bayer, E. (2025, April 30). A startup guide to selecting a Payment Service Provider. https://primer.io/blog/startup-payment-service-provider-guide

[537] MetaComp. (2025). Rise of stablecoins in Cross-Border Payments for ASEAN SMEs - MetaComp. In MetaComp. https://www.mce.sg/metacomp-whitepaper-cross-border-payments-for-smes-voices-in-asean-and-the-rise-of-stablecoins/

[538] Grand View Research. (2025). Europe cross border payments market size & outlook, 2030. Grand View Research. Retrieved September 28, 2025, https://www.grandviewresearch.com/horizon/outlook/cross-border-payments-market/europe

[539] Mordor Intelligence. (2025, June 23). Europe real time payments market size & share analysis: Growth trends & forecasts (2025 - 2030). https://www.mordorintelligence.com/industry-reports/europe-real-time-payments-market

[540] Mordor Intelligence. (2025, July 2). Europe payments market size & share analysis: Growth trends & forecasts (2025-2030). https://www.mordorintelligence.com/industry-reports/europe-payments-market

[541] Cipollone, P. (2025, May 15). Harnessing the digital future of payments: Europe's path to sovereignty and innovation. European Central Bank. https://www.ecb.europa.eu/press/key/date/2025/html/ecb.sp250515~fd8adac5a4.en.html

[542] Payten. (n.d.). POS related services & solutions. Retrieved September 28, 2025, https://www.payten.com/en/offers/for-merchants/pos-related-services-and-solutions/

[543] BR-DGE. (2025). Payments 101: Balancing volume in payments. Retrieved September 28, 2025, https://br-dge.to/blogs/payments-101-balancing-volume-in-payments/

[544] SMEs. (n.d.). https://www.pelicanpay.com/solutions/smes

[545] IXOPAY. (2025). Reduce your payment processing costs with a multi-PSP strategy. Retrieved September 28, 2025, https://www.ixopay.com/products/payment-orchestration/connectivity

[546] MarketPlace.commercetools. (2023). Gr4vy | marketplace.commercetools. Retrieved September 28, 2025, https://marketplace.commercetools.com/integration/gr4vy

Publisher Center for Digital Technology and Management
Arcisstr. 21
80333 Munich, Germany

E-Mail: info@cdtm.com
www.cdtm.com

Editors Vera Eger, Raunaq Jain

Team Heads Malte Oberhoff (Editing)
Karolina Wick (Quality Assurance)
Katy Grossmann (Layout)
Danit Niwattananan (Sources & Abbreviations)
Hanano Shiga (Marketing & Communication)
With support from the entire Class Fall 2025

Printed Copies 50

Printing Company printworld.com GmbH
Weststraße 60
09603 Großschirma

Photos https://unsplash.com/
https://www.stock.adobe.com/de/
https://www.gettyimages.de/
https://www.freepik.com/

Year of Publication 2025

THE FUTURE OF DIGITAL SOVEREIGNTY

Europe is at a tipping point. The foundations of tomorrow's digital world, such as cloud computing, artificial intelligence, and data infrastructure, are overwhelmingly controlled by non-European powers. This strategic dependency leaves Europe economically vulnerable, technologically constrained, and unable to fully protect the democratic values at the heart of its identity. Recent developments have highlighted the fragility of this position. Technology has become a powerful tool in international negotiations, with global platforms increasingly aligning with national political interests. Meanwhile, traditional allies can no longer be assumed to share Europe's strategic priorities. In this context, reliance on external powers poses a direct risk to Europe's economic resilience and political autonomy. Europe has the opportunity to shape its own path in building digital ecosystems that are resilient and grounded in European principles. After all, who builds the technology determines which values are encoded within it. Regulatory milestones such as the GDPR and the AI Act have already demonstrated Europe's ability to shape global standards. But is setting the rules enough if we do not control the underlying digital platforms? Can we truly claim to govern ourselves if our critical infrastructure and most innovative enterprises are hosted on servers and algorithms beyond our reach? The next step must be bolder: transforming regulatory strength into technological capability, and ambition into concrete innovation. Digital sovereignty, Europe's ability to act independently in the digital world, is intrinsically linked to economic prosperity, social cohesion, and democratic self-determination. It determines how Europe will compete, govern, and guard its liberties in an increasingly fractured world. By advancing on these fronts, Europe can evolve from dependency and establish itself as a leader of the digital era. This report examines how Europe can secure its digital sovereignty and translate this challenge into a structured path forward. It begins with a comprehensive analysis of the technological, societal, economic, legal, and environmental forces reshaping the digital sphere and defining Europe's position within it. Building on this foundation, the exploration section identifies five opportunity spaces, and the Ideation section transforms these opportunities into tangible concepts for business and policy, transitioning from analysis to inspiration and concrete action. Together, the three parts progress from understanding today's dynamics to outlining how a sovereign digital future can be built in practice.

CDTM

The Center for Digital Technology and Management (CDTM) is a joint interdisciplinary institution of education, research, and entrepreneurship of the Ludwig Maximilian University (LMU) and the Technical University of Munich (TUM).

CDTM offers the interdisciplinary certificate program "Technology Management". Students from various study backgrounds with creative ideas, great motivation and an entrepreneurial mindset are offered the tools to put their ideas into practice. As a research institution, CDTM closely cooperates with the industry, startups and the public sector concentrating on topics at the intersection of technology, innovation, and entrepreneurship.

E-mail info@cdtm.com
Website www.cdtm.com

Vera Eger, Raunaq Jain